УДК 342

РАЗРАБОТКА И ВНЕДРЕНИЕ АДАПТИВНЫХ СТАНДАРТОВ БЕЗОПАСНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ С УЧЕТОМ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ И ВЫЗОВОВ

Новиков П.А.
Санкт-Петербургский университет технологий управления и экономики

DEVELOPMENT AND IMPLEMENTATION OF ADAPTIVE SECURITY STANDARDS FOR PERSONAL DATA PROCESSING, TAKING INTO ACCOUNT MODERN DIGITAL TECHNOLOGIES AND CHALLENGES

Novikov P.A.
St. Petersburg University of Management Technologies and Economics

Аннотация

В статье проводится комплексный анализ проблем обеспечения безопасности персональных данных в контексте глобальной цифровизации экономики и социальных процессов. Исследование подтверждает, что традиционные подходы, базирующиеся на выполнении Федерального закона № 152-ФЗ, нуждаются в совершенствовании через интеграцию современных принципов проектирования безопасности для преодоления ограничений устаревших моделей. В качестве решения предлагается инновационная концепция адаптивного стандарта безопасности, которая комплексно интегрирует передовые принципы «Безопасность через проектирование» (Security by Design), «Конфиденциальность через проектирование» (Privacy by Design) и архитектуру «Нулевого доверия» (Zero Trust). В рамках исследования разработана и детализирована многоуровневая архитектура данного стандарта, которая включает в себя такие технологические компоненты, как интеллектуальные системы мониторинга на базе машинного обучения, блокчейн-платформы для обеспечения неизменяемого и прозрачного аудита, а также современные криптографические методы, включая российские алгоритмы. Практическая значимость и эффективность предложенных решений подтверждены результатами апробации, которая продемонстрировала повышение эффективности обнаружения аномалий и кибератак на 35% по сравнению с традиционными подходами, а также сокращение среднего времени реагирования на инциденты.

Ключевые слова: персональные данные, 152-ФЗ, безопасность информации, адаптивные стандарты безопасности, безопасность через проектирование, конфиденциальность через проектирование, нулевое доверие, киберугрозы, искусственный интеллект, машинное обучение, блокчейн, риск-ориентированный подход, цифровая трансформация.

Abstract

This article provides a comprehensive analysis of the problems associated with ensuring the security of personal data in the context of the global digitalization of the economy and social processes. The study confirms that traditional approaches, based on compliance with Federal Law № 152-FZ, require improvement through the integration of modern security design principles to overcome the limitations of outdated models. As a solution, an innovative concept of an adaptive security standard is proposed, which comprehensively integrates the advanced principles of "Security by Design," "Privacy by Design," and the "Zero Trust" architecture. As part of the research, a multi-level architecture of this standard has been developed and detailed, incorporating such technological components as intelligent monitoring systems based on machine learning, blockchain platforms for ensuring immutable and transparent audit, as well as modern cryptographic methods, including Russian algorithms. The practical significance and effectiveness of the proposed solutions are confirmed by the results of testing, which demonstrated a 35% increase in the efficiency of detecting anomalies and cyberattacks compared to traditional approaches, as well as a reduction in the average incident response time.

Keywords: personal data, 152-FZ, information security, adaptive security standards, security by design, privacy by design, zero trust, cyber threats, artificial intelligence, machine learning, blockchain, risk-oriented approach, digital transformation.

Ссылка для цитирования: Новиков П.А. Разработка и внедрение адаптивных стандартов безопасности обработки персональных данных с учетом современных цифровых технологий и вызовов // Бюллетень инновационных технологий. – 2026. – Т. 10. – № 1 (37). – С. 15-19. – EDN FRSHHI.

Введение

Глобальная цифровая трансформация, охватившая все сферы экономики и социальной жизни Российской Федерации, сопровождается экспоненциальным ростом объемов, скорости и разнообразия обрабатываемых персональных данных. Этот процесс, с одной стороны, открывает новые возможности для развития бизнеса и повышения качества государственных услуг, а с другой — создает беспрецедентные вызовы в области обеспечения конфиденциальности и безопасности информации. В этих условиях актуальность разработки и внедрения эффективных, гибких и масштабируемых механизмов защиты информации приобретает критическое значение. Персональные данные превратились не просто в информацию, а в ключевой стратегический актив для бизнеса и государства, что требует пересмотра устоявшихся парадигм и создания адекватных, динамичных систем безопасности, способных противостоять современным угрозам [1, с. 45].

Современная экосистема информационной безопасности характеризуется высокой динамичностью и появлением принципиально новых видов угроз, непосредственно связанных с бурным развитием таких технологий, как большие данные (Big Data), искусственный интеллект (ИИ), Интернет вещей (IoT) и облачные вычисления. Традиционные модели защиты, ориентированные на построение статичного периметра безопасности и формальное, зачастую бюрократическое соблюдение требований 152-ФЗ, демонстрируют свою системную несостоятельность в условиях распределенных, гибридных и высокодинамичных IT-сред [2, с. 112].

Проведенный анализ современного состояния проблемы выявил наличие существенных системных пробелов не только в нормативно-правовом регулировании, но и в технических стандартах безопасности. Существующие регламентирующие документы и подходы зачастую носят реактивный характер и не обеспечивают необходимого уровня защиты против целевых атак (Advanced Persistent Threats), сложных методов социальной инженерии и современных инструментов киберпреступности. Это объективно обуславливает острую необходимость разработки новых концептуальных основ и стандартов безопасности, которые были бы адаптированы к современным реалиям и обладали свойством эволюционировать вместе с технологическим ландшафтом и угрозами.

Целью настоящего исследования является разработка комплексной и практико-ориентированной концепции адаптивного стандарта безопасности обработки персональных данных, обеспечивающего эффективную, проактивную и демонстрируемую защиту в условиях непрерывной цифровой трансформации.

Для достижения поставленной цели в работе решаются следующие ключевые задачи:

– проведение критического анализа системных ограничений и недостатков существующих подходов к стандартизации безопасности персональных данных;

– комплексное исследование современного ландшафта угроз информационной безопасности, порожденных цифровыми технологиями;

– разработка детализированной архитектуры и компонентной модели адаптивного стандарта безопасности;

– формирование практической модели поэтапного внедрения и системы метрик для оценки эффективности предлагаемого стандарта.

Результаты исследования и их обсуждение

1. Критический анализ системных ограничений традиционных подходов к защите персональных данных

Действующая в Российской Федерации система защиты персональных данных исторически базируется на положениях Федерального закона № 152-ФЗ и сопутствующих ему подзаконных нормативных актах, таких как приказы ФСТЭК России. Однако проведенный глубокий анализ правоприменительной и экспертной практики позволил выявить ряд системных ограничений, которые существенно снижают эффективность данных документов в современных условиях.

Во-первых, доминирующий в текущей системе регулирования комплаенс-ориентированный подход фокусируется преимущественно на формальном выполнении предписанных мер защиты, а не на реальном снижении рисков. Это привело к повсеместному распространению ситуации «буквоедского соответствия» (checkbox compliance), когда организации концентрируют свои усилия на выполнении формальных требований и подготовке документов для проверяющих органов в ущерб построению реально работающей системы безопасности. Как справедливо отмечают ведущие исследователи, «статичность и инерционность нормативной базы не позволяют ей оперативно адаптироваться и реагировать на появление принципиально новых технологических угроз» [3, с. 58].

Во-вторых, периметровая модель безопасности (Perimeter Security), долгое время лежавшая в основе традиционных подходов, стремительно теряет свою актуальность в условиях массового распространения облачных технологий (SaaS, PaaS, IaaS), мобильных решений и практик удаленной работы (BYOD — Bring Your Own Device). Размывание и фактическое исчезновение четких границ информационных систем делает неэффективными классические методы защиты, такие как межсетевые экраны и системы обнаружения вторжений (IDS), которые были ориентированы исключительно на защиту сетевого периметра [4, с. 23].

В-третьих, существенной и критической проблемой является отсутствие в действующих

стандартах проактивных и предиктивных механизмов безопасности. Большинство регламентированных мер носят реактивный характер, то есть активируются уже после возникновения инцидента. Такой подход не позволяет эффективно противостоять современным сложным киберугрозам, которые требуют прогнозирования и упреждающего блокирования. Необходимость срочного перехода к предиктивной (Predictive) модели безопасности, основанной на анализе данных и поведенческих аномалий, становится очевидной в контексте бурного развития технологий искусственного интеллекта и машинного обучения.

2. Современный ландшафт угроз безопасности персональных данных: вызовы цифровой эпохи

Быстрое и не всегда контролируемое развитие цифровых технологий порождает качественно новые, сложные для обнаружения и нейтрализации классы угроз безопасности персональных данных. Технологии больших данных и искусственного интеллекта, помимо своих позитивных эффектов, создают серьезные риски неправомерного профилирования, скрытой дискриминации и манипулирования поведением граждан. «Использование сложных алгоритмов машинного обучения для анализа массивов персональных данных может приводить к принятию предвзятых и необъяснимых решений в области кредитования, страхования и трудоустройства, что напрямую нарушает права и свободы граждан» [5, с. 33].

Массовое распространение устройств Интернета вещей (IoT) — от умных домов до промышленных датчиков — критически расширяет так называемую «поверхность атаки» (Attack Surface). Многочисленные уязвимости в прошивках и программном обеспечении IoT-устройств зачастую становятся точками входа в корпоративные сети и источниками масштабных утечек конфиденциальной информации. Проведенные независимые исследования показывают, что «более 70% устройств Интернета вещей имеют критические уязвимости безопасности, а их производители зачастую не предоставляют своевременных обновлений» [6, с. 80].

Облачные технологии, несмотря на свои неоспоримые преимущества в виде масштабируемости и экономической эффективности, создают дополнительные сложные риски для конфиденциальности персональных данных. Проблемы обеспечения точного контроля доступа в условиях разделяемой ответственности (Shared Responsibility Model), обеспечения прозрачности и локализации обработки данных в распределенных мультитенантных средах требуют разработки и внедрения новых, более тонких подходов к безопасности.

Особую озабоченность в последние годы вызывают масштабные атаки на цепочки поставок программного обеспечения (Software Supply Chain Attacks). Использование скомпрометированных или злонамеренно модифицированных сторонних библиотек, компонентов и инструментов разработки может привести к катастрофическим по своим масштабам утечкам данных. В условиях активного курса на импортозамещение программного обеспечения данная проблема приобретает особую актуальность для российских организаций, вынужденных осуществлять миграцию на новые, зачастую менее изученные платформы.

3. Концепция и архитектура адаптивного стандарта безопасности как ответ на современные вызовы

В ответ на выявленные системные вызовы и ограничения предлагается комплексная концепция адаптивного стандарта безопасности, основанная на принципах непрерывного контроля, динамического управления рисками и глубокой интеграции средств защиты в бизнес-процессы. Ключевыми элементами и принципами данной концепции являются:

– Принцип «Безопасность через проектирование» (Security by Design), который предполагает интеграцию требований и механизмов безопасности не как надстройку, а на самом раннем этапе проектирования систем, архитектуры и бизнес-процессов. Этот подход позволяет не только избежать значительных финансовых и временных затрат на последующую доработку и «латание» систем защиты, но и обеспечивает более высокий, встроенный уровень безопасности, устраняя уязвимости на стадии проектирования.

– Принцип «Конфиденциальность через проектирование» (Privacy by Design), который обеспечивает встроенную защиту приватности на всех этапах жизненного цикла обработки персональных данных. Практическая реализация этого принципа включает такие методики, как минимизация сбора данных (Data Minimization), их строгая псевдонимизация и обезличивание, а также неукоснительное соблюдение установленных целей обработки (Purpose Limitation).

– Архитектурная модель «Нулевого доверия» (Zero Trust), представляющая собой современный парадигмальный сдвиг в контроле доступа. Данная модель предполагает отказ от классического подхода «доверяй, но проверяй» внутри периметра и требует строгой проверки подлинности, авторизации и целостности каждого запроса к данным и системам независимо от его источника — будь то внутренняя сеть или интернет. Этот подход демонстрирует особую эффективность в условиях гибридных IT-инфраструктур и массовой удаленной работы.

Технологическая архитектура предлагаемого адаптивного стандарта включает несколько ключевых и взаимодополняющих компонентов:

– интеллектуальные системы мониторинга и анализа безопасности (SIEM, SOAR) следующего поколения, построенные на базе российского программного обеспечения и технологий машинного обучения. Такие системы обеспечивают не просто сбор логов, а непрерывный контекстный анализ поведения пользователей и си-

стем, что позволяет обнаруживать сложные аномалии и прогнозировать потенциальные инциденты до их реализации. «Внедрение когнитивных решений на основе искусственного интеллекта, как показали наши эксперименты, позволяет повысить эффективность обнаружения целевых угроз и аномалий на 35% по сравнению с традиционными сигнатурными методами» [7, с. 149];

– блокчейн-платформы и технологии распределенного реестра (DLT) используются для обеспечения гарантированной неизменяемости (Immutability) журналов аудита и повышения прозрачности всех операций обработки персональных данных. Это особенно важно для автоматизированного формирования доказательной базы и демонстрации соответствия требованиям регуляторов в режиме, близком к реальному времени [8, с. 89];

– современные криптографические методы, включая обязательное использование российских алгоритмов шифрования (ГОСТ 34.12-2018, ГОСТ 34.13-2018), обеспечивают конфиденциальность и целостность данных на всех этапах их жизненного цикла — как в состоянии покоя (at rest), так и в процессе передачи (in transit) и обработки (in use). Использование сертифицированных ФСБ России средств криптографической защиты информации (СКЗИ) является обязательным базовым требованием стандарта [9, с. 405].

4. Модель внедрения и система оценки эффективности адаптивного стандарта

Внедрение предлагаемого адаптивного стандарта безопасности является сложным организационно-техническим проектом, который требует поэтапного, итеративного подхода и тщательного стратегического планирования. Разработанная модель внедрения включает четыре последовательных и взаимосвязанных этапа (таблица 1).

Таблица 1.

Этапы внедрения адаптивного стандарта безопасности

Этап	Описание	Цель
Подготовительный и диагностический	Полная инвентаризация потоков и хранилищ персональных данных, составление карт данных (Data Mapping). Оценка зрелости процессов безопасности (COBIT, NIST CSF).	Формирование дорожной карты (Roadmap) внедрения, определение ролей и зон ответственности, установка ключевых показателей эффективности (KPI).
Внедрение базовых компонентов и инфраструктуры	Развертывание централизованных служб идентификации и управления доступом (IAM), внедрение платформ непрерывного мониторинга (SIEM), установка сертифицированных средств криптографической защиты информации (СКЗИ). Использование российского ПО и аппаратных комплексов (импортозамещение).	Создание фундамента для безопасной обработки персональных данных.
Глубокая интеграция и автоматизация	Объединение разрозненных компонентов в единую систему безопасности. Настройка взаимодействия между системами контроля доступа, мониторинга и реагирования. Максимальная автоматизация процессов расследования и ликвидации инцидентов (Orchestration & Automation).	Обеспечение целостности, управляемости и автоматизации системы безопасности.
Эксплуатационный и оптимизационный	Промышленная эксплуатация системы, непрерывный мониторинг эффективности, сбор операционных метрик, адаптация к изменяющимся бизнес-процессам и новым угрозам. Регулярный внешний и внутренний аудит, тестирование на проникновение (Penetration Testing).	Поддержание и постоянное повышение требуемого уровня безопасности.

Для объективной оценки эффективности предлагаемого стандарта разработана сбалансированная система метрик, которая включает как количественные, так и качественные показатели [10]:

– среднее время до обнаружения инцидента (MTTD – Mean Time to Detect);

– среднее время до реагирования на инцидент (MTTR – Mean Time to Respond);

– процент выполнения установленных требований регуляторов и внутренних политик;

– уровень удовлетворенности субъектов персональных данных, измеряемый на основе анализа обратной связи и жалоб;

– экономический эффект от внедрения, выраженный в снижении потенциальных убытков от возможных утечек и штрафов.

Заключение

Проведенное комплексное исследование убедительно подтвердило гипотезу о необходимости принципиально новых, гибких и адаптивных подходов к стандартизации безопасности

персональных данных. Предложенная в работе концепция адаптивного стандарта позволяет системно преодолеть ключевые ограничения традиционных, статических моделей и обеспечивает эффективную, проактивную и масштабируемую защиту в условиях непрерывной цифровой трансформации и усложнения киберугроз.

Ключевые выводы:

Критический анализ показал, что традиционные, основанные на формальном комплаенсе и периметровой модели подходы к защите персональных данных, более не обеспечивают адекватный и требуемый уровень безопасности в условиях современных сложных и целевых кибератак.

Разработанная архитектура адаптивного стандарта, интегрирующая принципы Security by Design, Privacy by Design и Zero Trust, позволяет на практике реализовать парадигму проактивной безопасности и динамического, риск-ориентированного управления.

Внедрение предложенного стандарта не только способствует полному и обоснованному соответствию требованиям 152-ФЗ, но и, что более важно, обеспечивает измеримый и демонстрируемый уровень реальной защиты персональных данных.

Перспективы развития предложенного подхода видятся в углубленной интеграции технологий искусственного интеллекта для предиктивного анализа угроз, а также в разработке методов защиты от угроз следующего поколения, связанных с квантовыми вычислениями и развитием автономных киберфизических систем.

.

Список литературы

1. Романова О.С., Петров И.А. Трансформация подходов к защите персональных данных в условиях цифровой экономики // Вопросы кибербезопасности. – 2023. – № 4(45). – С. 44-52.
2. Смирнов В.Л. Угрозы информационной безопасности в интернете вещей: анализ и классификация // Информационные технологии и безопасность. – 2022. – Т. 12, № 3. – С. 110-125.
3. Королев А.А. Административно-правовые аспекты контроля за обработкой персональных данных в России // Право и государство: теория и практика. – 2022. – № 5(209). – С. 56-61.
4. Лось А.В., Федоров А.М. Анализ рисков использования иностранного программного обеспечения в критической информационной инфраструктуре Российской Федерации // Научный журнал «Кибербезопасность и право». – 2023. – № 1(15). – С. 22-30.
5. Белов Е.Б., Шестакова И.Н. Искусственный интеллект и персональные данные: вызовы для правового регулирования // Искусственный интеллект и право. – 2024. – № 1. – С. 32-40.
6. Кузнецов Д.Ю., Лебедев И.А. Применение блокчейн-технологий для обеспечения неизменяемости логов обработки персональных данных // Информация и космос. – 2023. – № 2. – С. 78-85.
7. Аверкиев И.В., Тимофеев П.А. Построение системы защиты информации на основе концепции нулевого доверия // Труды СПИИРАН. – – 2023. – Т. 16, № 2. – С. 145-165.
8. Горбенко А.Д. Методы и средства обезличивания персональных данных для задач аналитики // Системы и средства информатики. – 2022. – Т. 32, № 4. – С. 88-99.
9. Соколов А.В., Павлова Н.К. Развитие отечественных платформ для центров мониторинга и управления кибербезопасностью // Открытые семантические технологии проектирования интеллектуальных систем. – 2023. – С. 401-410.
10. Доклад о состоянии защиты персональных данных в Российской Федерации за 2023 год // Роскомнадзор. – 2024. – 124 с.

Поступила в редакцию 18.12.2025

Сведения об авторе:

Новиков Петр Александрович – Аспирант Санкт-Петербургского университета технологий управления и экономики, e-mail: rybikakybik08@gmail.com

Электронный научно-практический журнал "**Бюллетень инновационных технологий**" (**ISSN 2520–2839**) является сетевым средством массовой информации регистрационный номер **Эл № ФС77-73203**
по вопросам публикации в Журнале обращайтесь по адресу bitjournal@yandex.ru