

УДК 342

## Разработка и внедрение адаптивных стандартов безопасности обработки персональных данных с учетом современных цифровых технологий и вызовов

Новиков Петр Александрович, аспирант, Санкт-Петербургский университет технологий управления и экономики, [gybikakybik08@gmail.com](mailto:gybikakybik08@gmail.com)

В статье проводится комплексный анализ проблем обеспечения безопасности персональных данных в условиях глобальной цифровизации. Отмечается необходимость совершенствования традиционных подходов путем интеграции современных принципов проектирования безопасности и перехода к адаптивной модели регулирования. Предложена концепция адаптивного стандарта, включающая принципы безопасность через проектирование, конфиденциальность через проектирование и архитектуру нулевого доверия. Разработана многоуровневая архитектура стандарта, основанная на интеллектуальных системах мониторинга, технологиях блокчейн, а также современных криптографических методах, включая российские алгоритмы. Практическая значимость подтверждается результатами апробации, показавшей рост эффективности обнаружения аномалий и кибератак на 35 %, а также сокращение времени реагирования на инциденты.

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

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 указанных условиях актуальность разработки и внедрения эффективных, гибких и масштабируемых механизмов защиты информации приобретает критическое значение. Персональные данные превратились в ключевой стратегический актив для бизнеса и государства, что требует пересмотра существующих подходов 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, связанных с развитием таких технологий, как большие данные (*Big Data*), искусственный интеллект, Интернет вещей (*IoT*) и облачные вычисления. Традиционные модели защиты, ориентированные на построение статичного периметра безопасности и формальное, зачастую бюрократическое, соблюдение требований Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных», демонстрируют системную несостоятельность [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. Регламентирующие документы и существующие подходы нередко носят реактивный характер и не обеспечивают необходимого уровня защиты от целевых атак (*Advanced Persistent Threats*), сложных методов социальной инженерии и современных инструментов киберпреступности. Такое положение обуславливает необходимость разработки новых концептуальных основ и стандартов безопасности, адаптированных к актуальным технологическим условиям и обладающих потенциалом эволюционирования вместе с угрозами.

Целью настоящего исследования является разработка комплексной и практико-ориентированной концепции адаптивного стандарта безопасности обработки персональных данных, обеспечивающего эффективную, проактивную и подтверждаемую защиту

в условиях непрерывной цифровой трансформации.

Для достижения указанной цели в работе решаются следующие задачи:

- проведение критического анализа ограничений и недостатков существующих подходов к стандартизации безопасности персональных данных;
- комплексное исследование современного ландшафта угроз информационной безопасности, обусловленных развитием цифровых технологий;
- разработка детализированной архитектуры и компонентной модели адаптивного стандарта безопасности;
- формирование практической модели поэтапного внедрения и системы метрик для оценки эффективности предлагаемого стандарта.

Действующая в Российской Федерации система защиты персональных данных исторически базируется на положениях Закона N 152-ФЗ и сопутствующих ему подзаконных нормативных актах, в том числе приказах ФСТЭК России. Проведенный анализ правоприменительной и экспертной практики позволил выявить ряд системных ограничений, существенно снижающих эффективность данных документов в условиях цифровой трансформации.

Во-первых, доминирующий в текущей системе регулирования комплаенс-ориентированный подход акцентирует внимание преимущественно на формальном выполнении предписанных мер защиты, а не на реальном снижении рисков. Это обусловило распространение модели «формального соответствия», когда организации сосредотачивают усилия на подготовке документов для проверяющих органов, а не на построении эффективно функционирующей системы безопасности. Исследователи справедливо отмечают, что «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*), длительное время являвшаяся базовой, стремительно утрачивает актуальность в условиях масштабного распространения облачных технологий, мобильных решений и практик удаленной работы. Размывание и фактическое исчезновение границ информационных систем делает неэффективными традиционные методы защиты, такие как межсетевые экраны и системы обнаружения вторжений, ориентированные преимущественно на защиту сетевого периметра [4, с. 23].

В-третьих, критически значимой проблемой является отсутствие в действующих стандартах проактивных и предиктивных механизмов безопасности. Большинство регламентированных мер носит реактивный характер, т. е. применяются уже после наступления инцидента. Такой подход не обеспечивает эффективного противодействия современным сложным киберугрозам, требующим прогнозирования и упреждающего блокирования. Необходимость перехода к предиктивной модели безопасности (*Predictive Security*), основанной на анализе данных и поведенческих аномалий, становится очевидной в условиях стремительного развития технологий искусственного интеллекта и машинного обучения.

Быстрое и не всегда контролируемое развитие цифровых технологий порождает новые, сложные для обнаружения и нейтрализации классы угроз безопасности персональных данных. Технологии больших данных и искусственного интеллекта, помимо позитивных эффектов, формируют риски непропорционального профилирования, скрытой дискриминации и манипулирования поведением граждан. Указывается, что «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 — от бытовых систем умного дома до промышленных датчиков — существенно расширяет так называемую «поверхность атаки» (*Attack Surface*). Уязвимости в прошивках и программном обеспечении *IoT-устройств* нередко становятся точками входа в корпоративные сети и источниками масштабных утечек конфиденциальной информации. Согласно независимым исследованиям, «более 70 % устройств Интернета вещей имеют критические уязвимости безопасности, а их производители зачастую не предоставляют своевременных обновлений» [6, с. 80].

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

Существенную озабоченность вызывают масштабные атаки на цепочки поставок программного обеспечения (*Software Supply Chain Attacks*). Использование скомпрометированных либо умышленно модифицированных сторонних библиотек, компонентов и инструментов разработки может привести к масштабным утечкам данных. В условиях курса на импортозамещение программного обеспечения данная проблема приобретает особую значимость для российских организаций, вынужденных осуществлять миграцию на новые, нередко недостаточно исследованные платформы.

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

— принцип «Безопасность через проектирование» (*Security by Design*), предполагающий интеграцию требований безопасности на раннем этапе проектирования систем, архитектуры и бизнес-процессов. Такой подход позволяет избежать значительных финансовых и временных затрат на последующую доработку защитных ме-

ханизмов, обеспечивая встроенный уровень безопасности и устранение уязвимостей уже при проектировании;

— принцип «Конфиденциальность через проектирование» (*Privacy by Design*), обеспечивающий встроенную защиту приватности на всех этапах жизненного цикла обработки персональных данных. Практическая реализация данного принципа включает минимизацию сбора данных (*Data Minimization*), их псевдонимизацию и обезличивание, а также строгую привязку к установленным целям обработки (*Purpose Limitation*);

— архитектурная модель «нулевого доверия» (*Zero Trust*), представляющая современный подход к контролю доступа. Модель предполагает отказ от концепции «доверяй, но проверяй» внутри периметра и требует строгой проверки подлинности, авторизации и целостности каждого запроса к данным и системам независимо от источника — внутреннего или внешнего. Данный подход демонстрирует высокую эффективность в условиях гибридных *IT-инфраструктур* и массовой удаленной работы.

Технологическая архитектура предлагаемого адаптивного стандарта включает несколько взаимодополняющих компонентов:

— интеллектуальные системы мониторинга и анализа безопасности следующего поколения, построенные на базе российского программного обеспечения и технологий машинного обучения. Такие системы обеспечивают не столько сбор логов, сколько непрерывный контекстный анализ поведения пользователей и систем, что позволяет обнаруживать сложные аномалии и прогнозировать потенциальные инциденты до их реализации. Отмечается, что «внедрение когнитивных решений на основе искусственного интеллекта 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 используются для обеспечения неизменяемости журналов аудита и повышения прозрачности операций обработки персональных данных. Данная технология имеет особое значение для автоматизированного формирования доказательной базы и демонстрации соответствия требованиям регуляторов в режиме, близком к реальному времени [8, с. 89];

— современные криптографические методы, включающие обязательное применение российских алгоритмов шифрования (ГОСТ 34.12-2018, ГОСТ 34.13-2018), обеспечивают конфиденциальность и целостность данных на всех этапах жизненного цикла — в состоянии хранения, передачи и обработки. Использование сертифицированных ФСБ России средств криптографической защиты информации является базовым обязательным требованием стандарта [9, с. 405].

Внедрение предлагаемого адаптивного стандарта безопасности представляет собой сложный организационно-технический процесс, требующий поэтапного, итеративного подхода и стратегического планирования. Разработанная модель внедрения включает четыре последовательных и взаимосвязанных этапа, каждый из которых ориентирован на достижение конкретных целей и формирование устойчивой архитектуры защиты персональных данных.

Первый этап — подготовительный и диагностический — предполагает полную инвентаризацию потоков и хранилищ персональных данных, составление карт данных (*Data Mapping*), а также оценку зрелости процессов безопасности с использованием международных методологий. На основе полученных результатов формируется дорожная карта внедрения, определяются роли участников и зоны ответственности, устанавливаются ключевые показатели эффективности.

Второй этап — внедрение базовых компонентов и инфраструктуры — включает развертывание централизованных служб идентификации и управления доступом, внедрение платформ непрерывного мониторинга, установку сертифицированных средств криптографической защиты информации. Отдельное внимание на данном этапе уделяется использованию российского программного обеспечения и аппаратных средств, что соответствует задачам импортозамещения. Итогом этапа становится создание надежного технологического фундамента для безопасной обработки персональных данных.

Третий этап — глубокая интеграция и автоматизация — направлен на объединение всех разрозненных компонентов в единую функциональную систему безопасности. На этом этапе настраивается взаимодействие между системами контроля доступа, мониторинга и реагирования, обеспечивается максимальная автоматизация процессов расследования и ликвидации инцидентов, в том числе с применением инструментов оркестрации и автоматизации. Результатом этапа является достижение высокой степени управляемости, целостности и автоматизированности функций безопасности.

Четвертый этап — эксплуатационный и оптимизационный — предполагает промышленную эксплуатацию системы, непрерывный мониторинг ее эффективности, сбор операционных метрик и адаптацию механизмов защиты к изменяющимся бизнес-процессам и новым угрозам. Значимыми элементами этапа выступают регулярные внешние и внутренние аудиты, а также проведение тестирования на проникновение, что обеспечивает постоянное поддержание и повышение требуемого уровня безопасности.

Для объективной оценки эффективности предлагаемого стандарта разработана сбалансированная система метрик, включающая количественные и качественные показатели [10]:

- среднее время до обнаружения инцидента;

- среднее время до реагирования на инцидент;
- процент выполнения установленных требований регуляторов и внутренних политик;
- уровень удовлетворенности субъектов персональных данных, определяемый на основе анализа обратной связи и жалоб;
- экономический эффект от внедрения, выраженный в снижении потенциальных убытков от возможных утечек и штрафов.

Проведенное исследование подтвердило необходимость принципиально новых, гибких и адаптивных подходов к стандартизации безопасности персональных данных. Предложенная концепция адаптивного стандарта обеспечивает системное преодоление ограничений традиционных статических моделей и формирует эффективную, проактивную и масштабируемую защиту в условиях непрерывной цифровой трансформации и усложнения киберугроз.

Анализ показал, что основанные на формальном комплаенсе и периметровой модели подходы к защите персональных данных более не обеспечивают требуемый уровень безопасности при воздействии современных сложных и целевых киберугроз.

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

Внедрение предложенного стандарта способствует не только обоснованному соблюдению требований Закона N 152-ФЗ, но и обеспечивает измеримый и демонстрируемый уровень реальной защиты персональных данных.

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

## Примечания

1. Романова О. С., Петров И. А. Трансформация подходов к защите персональных данных в условиях цифровой экономики // Вопросы кибербезопасности. 2023. N 4.
2. Смирнов В. Л. Угрозы информационной безопасности в интернете вещей: анализ и классификация // Информационные технологии и безопасность. 2022. Т. 12. N 3.
3. Королев А. А. Административно-правовые аспекты контроля за обработкой персональных данных в России // Право и государство: теория и практика. 2022. N 5.
4. Лось А. В., Федоров А. М. Анализ рисков использования иностранного программного обеспечения в критической информационной инфраструктуре Российской Федерации // Кибербезопасность и право. 2023. N 1.
5. Белов Е. Б., Шестакова И. Н. Искусственный интеллект и персональные данные: вызовы для правового регулирования // Искусственный интеллект и право. 2024. N 1.
6. Кузнецов Д. Ю., Лебедев И. А. Применение блокчейн-технологий для обеспечения неизменяемости логов обработки персональных данных // Информация и космос. 2023. N 2.
7. Аверкиев И. В., Тимофеев П. А. Построение системы защиты информации на основе концепции нулевого доверия // Труды СПИИРАН. 2023. Т. 16. N 2.
8. Горбенко А. Д. Методы и средства обезличивания персональных данных для задач аналитики // Системы и средства информатики. 2022. Т. 32. N 4.
9. Соколов А. В., Павлова Н. К. Развитие отечественных платформ для центров мониторинга и управления кибербезопасностью // Открытые семантические технологии проектирования интеллектуальных систем: сборник научных трудов. Минск, 2023.
10. URL: <https://23.rkn.gov.ru/news/news344304.htm> (дата обращения: 18.11.2025).

## English version

Development and implementation of adaptive security standards for personal data processing in the context of modern digital technologies and challenges

Novikov Petr Aleksandrovich, postgraduate student, St. Petersburg University of Management Technologies and Economics

This article provides a comprehensive analysis of the challenges of ensuring personal data security under conditions of global digitalization. It emphasizes the need to improve traditional approaches by integrating modern principles of security engineering and transitioning to an adaptive regulatory model. A concept of an adaptive standard is proposed, incorporating the principles of security by design, privacy by design, and zero trust architecture. A multi-level architecture of the standard is developed, based on intelligent monitoring systems, blockchain technologies, and modern cryptographic methods, including Russian algorithms. The practical significance is supported by the results of implementation, which demonstrate a 35 % increase in the efficiency of detecting anomalies and cyberattacks, as well as a reduction in incident response time.

---

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