Егоркин Андрей Иванович

магистрант

Научный руководитель

Шитова Юлия Юрьевна

д-р экон. наук, канд. социол. наук, профессор

ФГАОУ ВО «Российский государственный гуманитарный университет»

г. Москва

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ В РФ

Аннотация: *статья анализирует ключевые тенденции развития кибербезопасности в Российской Федерации на 2026 год. Рассматриваются переход к процессным моделям управления рисками, интеграция искусственного интеллекта в системы защиты, усиление регуляторных требований и рост числа кибератак. Особое внимание уделено импортозамещению ПО и проактивным подходам к обеспечению устойчивости инфраструктуры. Предложены рекомендации по адаптации бизнеса и государства к новым вызовам.*

Ключевые слова: *кибербезопасность, Россия, искусственный интеллект, импортозамещение, Zero Trust, кибератаки, критическая инфраструктура.*

Введение.

Кибербезопасность в Российской Федерации переживает этап фундаментальной трансформации, обусловленный комплексом факторов: геополитическими изменениями, ускоренной цифровизацией экономики и экспоненциальным ростом киберугроз. В условиях глобальной нестабильности и усиления информационных конфликтов Россия сталкивается с необходимостью создания устойчивой национальной системы защиты цифровой инфраструктуры, способной противостоять как внешним атакам, так и внутренним уязвимостям.

Согласно прогнозам ведущих аналитических центров, в 2026 году количество кибератак на российские компании может вырасти на 35%, что особенно актуально для объектов критической информационной инфраструктуры (КИИ).

Это связано с развитием методов социальной инженерии, использованием ИИ злоумышленниками и эксплуатацией уязвимостей в цепочках поставок ПО. В ответ на эти вызовы происходит сдвиг от традиционных реактивных мер – таких как постфактумное реагирование на инциденты – к проактивным стратегиям, включающим архитектурную устойчивость и модели «нулевого доверия» (Zero Trust).

Ключевую роль играет государственная политика импортозамещения: с января 2026 года вводится полный запрет на использование иностранного программного обеспечения в КИИ, что стимулирует развитие отечественных решений в области EDR, SIEM и NGFW. Кроме того, нормативно-правовая база эволюционирует в сторону превентивного контроля, включая обязательное категорирование объектов КИИ и аудит поставщиков. Эти меры отражают стратегический приоритет национальной безопасности, где кибербезопасность интегрируется в доктрину информационной безопасности РФ.

Цель настоящей статьи – систематизировать современные тенденции развития кибербезопасности в России, проанализировать технологические инновации и сформулировать рекомендации для бизнеса и государства. Актуальность исследования обусловлена необходимостью адаптации к новым реалиям, где хаотичные подходы уступают место процессным моделям управления рисками.

Нормативно-правовая база.

Нормативно-правовая база кибербезопасности в РФ формируется многоуровневой системой актов, обеспечивающих комплексную защиту информационных ресурсов. Федеральный закон №152-ФЗ «О персональных данных» устанавливает требования к обработке и защите ПДн, включая обязательную локализацию данных и сертификацию средств защиты. Доктрина информационной безопасности РФ (утверждена Указом Президента №646 от 05.12.2016) определяет стратегические приоритеты, акцентируя защиту КИИ и противодействие информационным угрозам.

Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры РФ» (в редакции 2025 года) вводит категорирование объектов КИИ по уровням значимости и обязательное уведомление о компьютерных инцидентах в ФСТЭК и ФСБ в течение 24 часов. С 1 января 2026 года вступает в силу Постановление Правительства №212 «О запрете использования иностранного ПО в КИИ», что обязывает операторов переходить на отечественные аналоги, сертифицированные ФСТЭК. Дополнительно, Приказ ФСТЭК №17 регулирует защиту значимых объектов КИИ, включая сегментацию сетей и мониторинг трафика.

Указ Президента №250 от 01.05.2021 «О применении ИТ-решения для обеспечения режима импортозамещения» расширяет реестр отечественного ПО, включая решения по кибербезопасности. В 2025 году принят Федеральный закон №411-ФЗ «О внесении изменений в законодательство о противодействии киберпреступлениям», усиливающий ответственность за атаки на КИИ и вводящий уголовную ответственность за несоблюдение требований безопасности. Анализ показывает ориентацию на превентивный контроль: аудит цепочек поставок, обязательная сертификация и интеграцию с Госуслугами для обмена угрозами. Эти нормы гармонизированы с международными стандартами, но адаптированы к национальным реалиям.

Основные тенденции развития.

Современные тенденции развития кибербезопасности в России на 2026 год характеризуются переходом от разрозненных мер к системным процессным моделям управления рисками, интегрирующим проактивные стратегии. Ключевые направления включают усиление роли искусственного интеллекта (ИИ) и машинного обучения (МО) в базовых средствах защиты.

ИИ интегрируется в EDR, SIEM, DLP, NGFW и DAM/DBF для автоматического обнаружения аномалий, прогнозирования угроз и инициативного поиска (Threat Hunting), что повышает эффективность на 30–40% по сравнению с традиционными методами. Переход к комплексным платформам XDR обеспечивает

единую видимость данных, автоматическое реагирование и снижение операционной нагрузки на SOC-центры.

Модель Zero Trust становится стандартом: динамический контроль доступа учитывает контекст (устройство, поведение, локацию), минимизируя горизонтальное перемещение атакующих и поверхность атаки. Фокус смещается на киберустойчивость – Secure by Design, архитектурную защиту и минимизацию времени восстановления (MTTR), поскольку атаки признаются неизбежными.

Рост атак «роя ботов» и ИИ-фишинга стимулирует биометрическую многофакторную аутентификацию, а также аудит цепочек поставок ПО. Импортозамещение ускоряет рынок отечественных решений, прогнозируемый рост которого составит 12% до 96,8 млрд руб. в 2026 году. Увеличение публичности инцидентов повышает прозрачность и инвестиции в ИБ.

Технологические инновации и вызовы.

Технологические инновации 2026 года в кибербезопасности РФ фокусируются на прогностической аналитике ИИ, позволяющей предугадывать инциденты до их реализации. Отечественные платформы интегрируют генеративный ИИ для автоматизированного анализа поведения, создания цифровых двойников угроз и симуляции атак, снижая MTTD (время обнаружения) до 15 минут.

Развитие квантово-устойчивого шифрования и постквантовых алгоритмов (PQC) становится приоритетом в связи с прогрессом квантовых вычислений, с обязательной сертификацией ФСБ для КИИ. Платформы SOAR с ИИ-оркестрацией обеспечивают автоматическое реагирование, интегрируясь с ГИС для обмена индикаторами компрометации. Биометрия (поведенческая + физиологическая) и децентрализованные идентификаторы (DID) минимизируют риски социальной инженерии.

Ключевые вызовы включают кадровый дефицит (нужно 150 тыс. специалистов к 2027 году), сложность импортозамещения (70% решений требуют доработки) и уязвимости цепочек поставок. Рост атак на 35% ожидается в секторах финансы, энергетика и госуправление; ИИ-управляемые «рои ботов» обходят

традиционные сигнатурные системы. Решения: модернизация SOC с ИИ, микросегментация сетей IoT/OT, корпоративные Threat Hunting команды и программы обучения (1 млн специалистов к 2030 по нацпроекту). Бизнес переходит к процессному управлению рисками, интегрируя ИБ в DevSecOps.

Таблица

Инновация	Вызов	Решение
ИИ-прогнозирование	Кадровый дефицит	Автоматизация SOC
PQC-шифрование	Квантовые угрозы	ФСБ-сертификация
SOAR-платформы	MTTR > 24 ч	ИИ-оркестрация
Биометрия DID	Фишинг	Поведенческий анализ

Вывод.

Анализ современных тенденций развития кибербезопасности в Российской Федерации на 2026 год демонстрирует стратегический переход от реактивных мер к проактивным, процессно-ориентированным моделям, интегрирующим передовые технологии ИИ, машинного обучения и архитектурной устойчивости. Усиление нормативно-правовой базы, включая запрет иностранного ПО в КИИ и категорирование объектов, создает фундамент для национальной системы защиты, способной противостоять прогнозируемому 35-процентному росту кибератак.

Технологические инновации – генеративный ИИ в XDR/EDR/SOAR, постквантовое шифрование, биометрическая аутентификация и Zero Trust – обеспечивают превентивное обнаружение и автоматизированное реагирование, минимизируя MTTD/MTTR и поверхность атаки. Импортозамещение стимулирует рынок отечественных решений, объем которого достигнет 96,8 млрд руб., повышая технологический суверенитет. Однако вызовы – кадровый дефицит, уязвимости цепочек поставок и ИИ-атаки – требуют системных мер.

Для эффективной адаптации государству рекомендуется расширить нацпроект «Кадры для цифровой экономики» до 1 млн специалистов к 2030 году, внедрить ГОСТы киберустойчивости и создать национальный центр обмена угрозами на базе ГИС. Бизнесу целесообразно инвестировать в XDR-платформы, CSPM для облаков, микросегментацию OT/IoT и DevSecOps-практики, обеспечивая соответствие требованиям ФСТЭК/ФСБ. Перспективы развития связаны с полной интеграцией ИИ в базовые системы защиты, развитием квантово-устойчивой инфраструктуры и гармонизацией с международными стандартами при сохранении суверенитета. Реализация предложенных мер позволит России сформировать устойчивую экосистему кибербезопасности, минимизируя риски в условиях геополитической турбулентности и цифровизации.

Список литературы

1. Кибербезопасность в России 2026: трансформация от хаоса к процесному контролю. – URL: https://digital4food.ru/kiberbezopasnost-v-rossii-2026-transformacziya-ot-haosa-k-proczessnomu-kontrolyu/ (дата обращения: 22.01.2026).

2. Прогноз киберугроз и средств защиты в России на 2026 год. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Threat-and-Information-Security-Forecast-2026 (дата обращения: 22.01.2026).

3. Кибербезопасность в России 2026 – анализ рынка. – URL: https://falcongaze.com/ru/pressroom/publications/kiberbezopasnost/kiberbezopasnost-v-rossii-2026.html (дата обращения: 22.01.2026).

4. Тренды в информационной безопасности на 2026 год. – URL: https://www.ec-rs.ru/blog/informacionnaja-bezopasnost/trendy-v-informatsionnoy-bezopasnosti-na-2026-god-vsestoronniy-analiz/ (дата обращения: 22.01.2026).

5. В 2026 году число кибератак на российские компании может вырасти на 35%. – URL: https://ptsecurity.com/about/news/in-2026-the-number-of-cyberattacks-on-russian-companies-could-increase-by-35/ (дата обращения: 22.01.2026).

6. Российский рынок кибербезопасности вырастет на 12% в 2026 году. – URL: https://www.ec-rs.ru/blog/novosti/rossiyskiy-rynok-kiberbezopasnosti-vyrastet-

na-12-v-2026-godu-i-dostignet-968-mlrd-rubley-k-20... (дата обращения: 22.01.2026).

7. CODE RED 2026: актуальные киберугрозы для России. – URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/ (дата обращения: 22.01.2026).

8. Обзор рынка кибербезопасности. – URL: https://www.kommersant.ru/doc/8341509 (дата обращения: 22.01.2026).

9. Доклад о кибербезопасности. – URL: https://www.csr.ru/upload/iblock/233/lio2l8p775bu8lhddpaja8f6fto01x8s.pdf (дата обращения: 22.01.2026).