Александрова Жанна Павловна

канд. социол. наук, доцент

Говорухина Мария Олеговна

бакалавр, студентка

Колодяжная Алиса Михайловна

бакалавр, студентка

ФГБОУ ВО «Кубанский государственный технологический университет»

г. Краснодар, Краснодарский край

СОВРЕМЕННЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ В УСЛОВИЯХ РОСТА ЦИФРОВЫХ УГРОЗ

Аннотация: *в статье рассматриваются ключевые вызовы в области защиты информации, вызванные экспоненциальным ростом объёмов данных и усложнением ландшафта киберугроз в 2023–2025 гг. Проанализированы современные подходы: архитектура нулевого доверия (Zero-Trust), конфиденциальные вычисления, гомоморфное шифрование, постквантовая криптография, технологии усиления конфиденциальности (Privacy-Enhancing Technologies) и принцип «приватность по умолчанию и по дизайну» (Privacy by Design). Особое внимание уделено практическим примерам внедрения и нормативному регулированию в России и мире.*

Ключевые слова: *информационная безопасность, конфиденциальность данных, zero-trust, гомоморфное шифрование, постквантовая криптография, Privacy by Design, цифровые угрозы.*

По данным отчёта Verizon Data Breach Investigations Report 2024, 68% инцидентов связаны с компрометацией учётных данных и человеческим фактором [5], а 83% атак затрагивают внешний периметр или облачные сервисы. По прогнозам Cybersecurity Ventures, ежегодные глобальные убытки от киберпреступности к 2025 году превысят 10,5 трлн долларов США [1]. Объём мировых

данных, согласно IDC, достигнет 181 зеттабайта в 2025 году [2]. Традиционные периметровые модели защиты (castle-and-moat) в таких условиях теряют эффективность, что требует перехода к новым архитектурным и криптографическим парадигмам.

За последние годы значительно выросло число атак на цепочки поставок (SolarWinds 2020, Log4Shell 2021, MOVEit 2023, XZ Utils 2024), увеличилось использование генеративного ИИ для автоматизации атак (FraudGPT, WormGPT, deepfake-фишинг), появились реальные квантовые угрозы (в 2024 году NIST опубликовал первые стандарты постквантовой криптографии ML-KEM, ML-DSA, SLH-DSA) [3], усилились атаки на среды доверенного выполнения (Spectre/Meltdown-подобные уязвимости в TEE).

Таблица 1

Современные архитектурные и технологические подходы

1. Архитектура нулевого доверия (Zero-Trust Architecture)	Принцип «никогда не доверяй, всегда проверяй» реализуется через непрерывную аутентификацию, микросегментацию и контекстно-зависимую авторизацию. Ведущие реализации: Google BeyondCorp, Microsoft Zero Trust Security Model, CrowdStrike Falcon Zero Trust
2. Конфиденциальные вычисления (Confidential Computing)	Технологии доверенной среды выполнения (Trusted Execution Environment, TEE): Intel SGX/TDX, AMD SEV-SNP, ARM Confidential Compute Architecture, NVIDIA Confidential GPUs. Практические продукты: Azure Confidential VMs, AWS Nitro Enclaves, Google Confidential VM. Обеспечивают защиту данных в процессе обработки даже от облачного провайдера
3. Гомоморфное шифрование	Позволяет выполнять вычисления над зашифрованными данными без их расшифровки. Современные библиотеки: Microsoft SEAL, IBM HElib, OpenFHE. Применяется в медицине и финансах для соблюдения GDPR, HIPAA и ФЗ-152 при аналитике чувствительных данных
4. Постквантовая криптография	С 2024 года начат глобальный переход на алгоритмы, стойкие к атакам на квантовых компьютерах: Kyber (ML-KEM), Dilithium (ML-DSA), Falcon, SPHINCS+ [3]. Google и Cloudflare уже внедряют гибридные схемы в TLS
5. Технологии усиления конфиденциальности (Privacy-Enhancing Technologies, PETs)	– дифференциальная приватность (Apple, Google, IBM); – федеративное обучение (TensorFlow Federated, PySyft); – синтетические данные (Mostly AI, Gretel.ai); – безопасные многопартийные вычисления (MP-SPDZ, ShareMind)

В условиях роста ИИ и квантовых угроз PETs интегрируются с блокчейном: Oasis Network и Phala Network сочетают TEE со смарт-контрактами для

вычислений над зашифрованными данными в здравоохранении и финансах. Гомоморфное шифрование ускоряется оборудованием: чипы NVIDIA/Intel снижают нагрузку на 50–70% vs Microsoft SEAL. В РФ «Цифровая экономика-2025» внедряет PETs в «Госуслуги» для биометрии. Однако вызовы остаются: высокая стоимость развертывания (до 10 раз дороже традиционных методов по данным Gartner 2025) и необходимость квалифицированных специалистов.

Нормативно-правовое обеспечение. В ЕС действуют GDPR (2018), AI Act (2024) [4] и готовится ePrivacy Regulation. В России – ФЗ-152 «О персональных данных» (ред. 2024) [7], ФЗ-187 «О безопасности КИИ», Указ Президента №250 от 01.05.2022 [6]. В США – CCPA/CPRA и секторальные законы, в Китае – PIPL (2021) и GB/T 42410–2023.

Современная информационная безопасность требует комплексного подхода к защите данных на всех стадиях: в покое, в движении и в процессе обработки. Наиболее перспективными направлениями являются архитектура нулевого доверия, конфиденциальные вычисления, гомоморфное шифрование, постквантовая криптография и технологии усиления конфиденциальности. Их интеграция с принципом Privacy by Design позволяет организациям эффективно противостоять текущим и будущим цифровым угрозам, сохраняя при этом соответствие строгим нормативным требованиям.

Список литературы

1. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. URL: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ (дата обращения: 14.01.2026).

2. Global DataSphere Forecast, 2021–2025. URL: https://www.idc.com/getdoc.jsp?containerId=US47509621 (дата обращения: 14.01.2026).

3. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (дата обращения: 14.01.2026).

4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. L 1689. 2024.

5. Verizon Data Breach Investigations Report 2024. Verizon, 2024. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата обращения: 14.01.2026).

6. Указ Президента Российской Федерации от 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. – URL: http://publication.pravo.gov.ru/Document/View/0001202205010023 (дата обращения: 14.01.2026).

7. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (в ред. от 08.08.2024) // СПС КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 14.01.2026).