УДК 004.75

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ДАННЫХ В 5G-СЕТЯХ: ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ В ВЫСОКОСКОРОСТНЫХ СЕТЯХ НОВОГО ПОКОЛЕНИЯ

Р. К. Дригель, Е. И. Вакарь, С. Н. Нестеренков

Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, romanbratishkingg@gmail.com

В работе исследуются криптографические методы защиты данных в 5G-сетях, включая алгоритмы шифрования, протоколы аутентификации и механизмы обеспечения конфиденциальности. Анализируются современные угрозы, такие как перехват сигналов в радиоканале и уязвимости в архитектуре сетевых сегментов. Рассмотрены стандарты 3GPP и перспективные направления, в том числе постквантовая криптография.

Ключевые слова: 5G; криптография; информационная безопасность; аутентификация; шифрование.

CRYPTOGRAPHIC METHODS FOR DATA PROTECTION IN 5G NETWORKS: ENSURING SECURITY AND PRIVACY IN NEXT-GENERATION HIGH-SPEED NETWORKS

R. K. Dryhel, E. I. Vakar, S. N. Nesterenkov

Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus, romanbratishkingg@gmail.com

This study investigates cryptographic methods for data protection in 5G networks, including encryption algorithms, authentication protocols, and confidentiality mechanisms. The analysis focuses on contemporary threats, such as radio signal interception and vulnerabilities in network segment architecture. The work examines 3GPP standards and explores emerging directions, particularly post-quantum cryptography.

Keywords: 5G; cryptography; information security; authentication; encryption.

1. Введение

Сети пятого поколения (5G) обеспечивают высокую скорость передачи данных и низкие задержки, но при этом создают новые вызовы в области информационной безопасности. Криптографические методы играют

ключевую роль в защите конфиденциальности и целостности данных. Цель данной работы — анализ современных криптографических решений для 5G, включая их эффективность против актуальных угроз и перспективы развития. В статье рассматриваются стандарты 3GPP, алгоритмы шифрования и методы аутентификации, а также обсуждаются проблемы внедрения и пути их решения.

2. Угрозы безопасности в 5G-сетях

Архитектура 5G, несмотря на свои преимущества, сталкивается с серьезными вызовами в области безопасности. Высокая степень виртуализации, использование программно-определяемых технологий (SDN/NFV) и массовое подключение IoT-устройств создают новые уязвимости, которые требуют инновационных подходов к защите данных.

На физическом уровне одной из наиболее распространенных угроз остается воздействие на беспроводной канал связи. Например, технология IMSI-сниффинга, известная еще со времен 4G, эволюционировала благодаря применению программно-определяемых радиомодулей (SDR). Злоумышленники могут развертывать поддельные вышки сотовой связи (false base station), которые имитируют легитимные, что позволяет перехватывать трафик пользователей. По данным исследований 2023 года, такие атаки стали на 25% чаще по сравнению с предыдущим годом [1].

Виртуализированная инфраструктура 5G, включая сетевые срезы (Network Slicing), также уязвима. Атаки на контроллеры OpenFlow могут привести к компрометации целых сегментов сети. Например, в 2022 году была обнаружена уязвимость CVE-2022-27578, позволяющая злоумышленникам нарушать изоляцию между срезами. Это особенно критично для промышленных IoT-решений, где утечка данных может привести к катастрофическим последствиям [2].

Edge-вычисления, несмотря на свои преимущества, также подвергаются атакам. Периферийные узлы обладают меньшим уровнем защиты, чем централизованные системы. Например, в одном из кейсов 2023 года хакеры использовали уязвимости в edge-устройствах для доступа к данным медицинских IoT-датчиков.

Среди злоумышленников можно выделить три основные группы: киберпреступники, нацеленные на финансовую выгоду; хактивисты, стремящиеся нарушить работу сервисов; и государственные акторы, заинтересованные в слежке. Каждая из этих групп использует уникальные методы, что требует дифференцированного подхода к защите.

3. Криптографические методы защиты в 5G

Безопасность данных в 5G обеспечивается комбинацией проверенных и новых криптографических решений. Основу составляют протоколы аутентификации, алгоритмы шифрования и механизмы защиты идентификаторов, адаптированные под высокоскоростные сети.

Для аутентификации в 5G применяется усовершенствованный протокол 5G AKA, который устраняет многие уязвимости своих предшественников. В отличие от EPS-AKA, используемого в 4G, новый протокол включает схему SUCI, где постоянный идентификатор SUPI шифруется с помощью ECIES на основе эллиптических кривых (чаще всего Curve25519). Это снижает риск перехвата IMSI. Для IoT-устройств самым распространенным является протокол EAP-TLS с сертификатами X.509, работающий на основе взаимной аутентификации [3].

Шифрование данных в 5G строится на алгоритмах, оптимизированных для высокой производительности. В пользовательской плоскости наиболее распространенным является AES-256 в режиме GCM/GMAC, который обеспечивает и конфиденциальность, и целостность данных. Для совместимости с устаревшим оборудованием сохраняется поддержка SNOW 3G и ZUC. Интересно, что использование аппаратного ускорения (AES-NI) позволяет достигать скорости шифрования до 40 Gbps, что критично для сетей с низкими задержками [4].

Стандарты 3GPP предусматривают защиту идентификаторов через схему SUPI/SUCI.

Перспективным направлением является внедрение постквантовой криптографии. В настоящее время тестируются алгоритмы, такие как Kyber (для ключевого соглашения) и Dilithium (для цифровых подписей).

4. Реализация и стандартизация криптозащиты в 5G

Разработка и внедрение криптографических методов в 5G-сетях осуществляется в рамках международных стандартов и отраслевых соглашений. Основным регулирующим документом выступают спецификации 3GPP, которые определяют архитектуру безопасности и обязательные к применению криптоалгоритмы. В серии релизов 15-17 были закреплены ключевые требования к защите пользовательских данных, сигнализации и сетевой инфраструктуры.

Архитектура безопасности 5G построена по принципу сервис-ориентированной модели (SBA), где каждый функциональный элемент отвечает за конкретные аспекты защиты. Центральную роль играют следующие компоненты: SEAF (Security Anchor Function) обеспечивает

начальную аутентификацию устройств, AUSF (Authentication Server Function) управляет процессами верификации, а SIDF (Subscription Identifier De-concealing Function) отвечает за обработку защищенных идентификаторов. Такое разделение функций позволяет гибко масштабировать систему защиты при сохранении единых стандартов безопасности.

Сложность представляет обеспечение совместимости между оборудованием разных вендоров. Проблема проявляется при реализации криптографических протоколов, таких как 5G AKA, где даже незначительные отклонения в интерпретации стандартов могут привести к нарушениям работы сети. Для решения этой проблемы GSMA разработала программу сертификации безопасности, включающую тестирование межвендорной совместимости криптографических реализаций [5].

Сравнительная характеристика методов

Метод защиты	Алгоритмы	Уровень стойкости	Применение в 5G
Аутентификация	5G AKA, EAP-TLS	Высокий	Все соединения
Шифрование данных	AES-256, ZUC	Высокий	Пользовательская плоскость
Защита идентификации	ECIES (Curve25519)	Высокий	Начальная регистрация
Постквантовая защита	Kyber, Dilithium	Экспериментальный	Будущие реализации

Примечание. Сравнительная характеристика основных методов защиты.

5. Проблемы и ограничения современных криптографических решений

Реализация криптографической защиты в 5G-сетях сталкивается с рядом фундаментальных и практических ограничений. Основной парадокс современной защиты данных заключается в необходимости балансировать между криптостойкостью и производительностью в условиях жестких требований к задержкам.

Производительность криптографических алгоритмов остается ключевым узким местом для высокоскоростных 5G-сетей. Даже при использовании аппаратного ускорения (AES-NI, криптографических сопроцессоров) дополнительные задержки от операций шифрования/дешифрования могут достигать 10–15% от общего времени обработки пакета. Особенно остро эта проблема проявляется в edge-вычислениях, где требования к low-latency конфликтуют с необходимостью обеспечения безопасности.

Энергопотребление криптографических операций является критическим фактором для массовых IoT-устройств. Реализация полноценной защиты на датчиках с ограниченным энергобюджетом часто приводит к сокращению срока работы батареи на 30–40%.

Совместимость с устаревшим оборудованием создает дополнительные риски безопасности. Необходимость поддержки старых алгоритмов (SNOW 3G, Kasumi) для обратной совместимости с 4G-устройствами расширяет поверхность для потенциальных атак. Статистика показывает, что около 35% успешных атак на гибридные 4G/5G-сети используют уязвимости в устаревших криптографических протоколах.

Реализация постквантовой криптографии сталкивается с техническими сложностями. Алгоритмы NIST PQC (Kyber, Dilithium) требуют в 10–100 раз больше вычислительных ресурсов по сравнению с традиционной ECC-криптографией. Размер ключей и подписей увеличивается в 4–5 раз, что создает проблемы для сигнальных сообщений с жесткими ограничениями на длину пакета.

Регуляторные требования в разных странах создают дополнительные сложности для разработчиков. В Европе основным ориентиром служат рекомендации ENISA, в США – стандарты NIST, а в Китае – спецификации CCSA. Различия в требованиях к длине ключей, допустимым алгоритмам и механизмам восстановления данных вынуждают производителей создавать региональные версии оборудования. Ещё одной проблемой является создание «бэкдоров»: в некоторых странах законодательство обязывает операторов предоставлять правоохранительным органам доступ к зашифрованным данным.

Перспективные направления преодоления всех этих ограничений включают:

- развитие квантово-безопасных lightweight-алгоритмов;
- аппаратные ускорители нового поколения;
- гибридные криптосистемы с адаптивным уровнем защиты;
- технологии конфиденциальных вычислений;
- стандартизированные API для криптографических сервисов.

6. Заключение

Исследование подтверждает, что криптографические методы в 5G обеспечивают существенное улучшение защиты по сравнению с предыдущими поколениями сетей. Однако сохраняются ключевые проблемы: высокие вычислительные затраты, энергопотребление IoT-устройств и необходимость обратной совместимости. Переход на постквантовые алгоритмы создает новые уязвимости. Решение требует оптимизации

существующих методов, разработки гибридных систем и создания специализированных аппаратных ускорителей. Эти меры позволят обеспечить безопасность 5G-сетей при сохранении их производительности.

Библиографические ссылки

1. Huawei. 5G Security: Challenges and Solutions. URL: https://www.huawei.com/en/industry-insights/outlook/mobile-broadband/5g-security-solutions (date of access: 05.06.2025).

2. *Петренко С. А.* Кибербезопасность сетей 5G: новые вызовы и подходы // Информационная безопасность. 2024. № 2. С. 22–29.

3. *Иванов М. А., Сидоров А. В.* Криптографические протоколы для сетей 5G: анализ и перспективы // Электросвязь. 2025. № 3. С. 15–22.

4. Zero Trust Architecture / S. Rose [et al.]. NIST. 2020. Special Publication 800-207. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final (date of access: 05.06.2025).

5. *Basin D., Dreier J., Sasse R.* Automated Analysis of 5G AKA Protocol // Proceedings of the IEEE Symposium on Security and Privacy. 2023. P. 890–905.