

УДК 004.056

DOI 10.26118/2818.2025.61.94.017

*Смирнов И.А., аспирант,
Московский институт электроники и математики
им. А.Н. Тихонова НИУ ВШЭ,
Россия, Москва
Smirnov I.A., graduate student,
HSE Tikhonov Moscow Institute of Electronics and Mathematics
Russia Moscow*

**Оценка эффективности мер по снижению киберрисков в сетях 5G:
практический подход к обеспечению безопасности цифровых экосистем
Evaluating the effectiveness of cyber risk mitigation measures in 5G
networks: a practical approach to securing digital ecosystems**

Аннотация. Исследование посвящено оценке эффективности мер по снижению киберрисков в сетях 5G. Рассмотрены ключевые уязвимости и угрозы, возникающие вследствие развития технологий искусственного интеллекта, анализа больших данных, Интернета вещей и робототехники. Проанализирована архитектура сетей 5G, выявлены основные угрозы кибербезопасности и разработаны рекомендации по их устранению. Проведен расчет показателей риска с использованием методологии CASE, демонстрирующий снижение вероятности реализации угроз на 20% и уменьшение их потенциального воздействия на 28%. Полученные результаты имеют практическую значимость для интернет-провайдеров и операторов связи, позволяя минимизировать риски кибербезопасности.

Ключевые слова: ИТ-2020, 5G, беспроводные технологии, уязвимости, архитектура, киберриски, CASE

Annotation. The study is devoted to assessing the effectiveness of measures to reduce cyber risks in 5G networks. The key vulnerabilities and threats arising from the development of artificial intelligence technologies, big data analysis, the Internet of Things and robotics are considered. The architecture of 5G networks is analyzed, the main cybersecurity threats are identified and recommendations for their elimination are developed. Risk indicators are calculated using the CASE methodology, demonstrating a 20% reduction in the probability of threat implementation and a 28% reduction in their potential impact. The results obtained are of practical importance for Internet providers and telecom operators, allowing them to minimize cybersecurity risks.

Key words IMT-2020, 5G, wireless technologies, vulnerabilities, architecture, cyber risks, CASE

Развитие информационно-коммуникационных технологий определяет современную цифровую экономику, где сети 5G играют ключевую роль, обеспечивая высокий уровень производительности, скорости передачи данных и надежности. Вместе с ростом возможностей возникают и новые вызовы в области информационной безопасности. Быстро развивающиеся технологии искусственного интеллекта (AI), машинного обучения (ML), анализа больших данных (Big Data), Интернета вещей (IoT) и робототехники повышают потребность в эффективных мерах защиты сетей 5G от кибератак. Современная архитектура сетей 5G представляет собой сложную систему, состоящую из множества компонентов, интегрированных друг с другом. Безопасность каждого элемента влияет на общий уровень защищенности всей сети, что повышает важность комплексного подхода к обеспечению информационной безопасности.

Основная цель настоящего исследования — оценка эффективности существующих мер минимизации выявленных рисков информационной безопасности в сетях 5G, а также разработка практических рекомендаций по их улучшению. Для достижения этой цели проводится глубокий анализ архитектуры сетей 5G, определяются ключевые угрозы и предлагаются конкретные меры, направленные на укрепление информационной безопасности.

Методологической основой исследования послужила подробная экспертиза архитектуры сетей 5G с точки зрения информационной безопасности. Для организации безопасной беспроводной сети 5G требуется провести анализ архитектуры с позиции информационной безопасности, чтобы предотвратить возможные риски реализации угроз при её дальнейшем использовании [1,2]. Общая архитектура 5G/IMT-2020, представленная на рис. 1, рассматривается в данной работе на основе данных из источников [3,4].

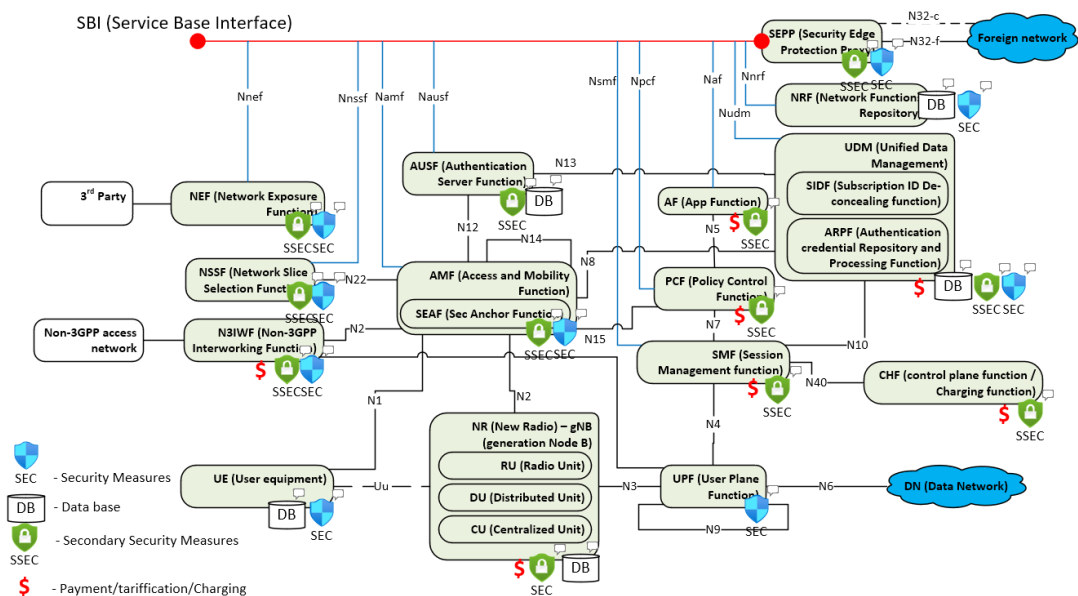


Рис. 1. Общая архитектура 5G/IMT-2020

Каждая из этих функций имеет свой уровень безопасности и защитные механизмы.

1. User Equipment (UE) – Аутентификация и авторизация пользователя. Защита пользовательских данных посредством шифрования и контроля целостности данных. Поддержка защиты от распространенных угроз, таких как поддельные базовые станции и мошеннические атаки.

2. Node B (gNB) – Проверка подлинности и шифрование передаваемых данных. Мониторинг и фильтрация потенциально опасного трафика. Контроль качества предоставления услуг и защиты доступа к ресурсам сети.

3. Network Repository Function (NRF) – Центральное хранение и предоставление информации о зарегистрированных сетевых функциях и их полномочиях. Механизмы авторизации и аутентификации для подтверждения легитимности сетевых запросов. Фильтрация белого и черного списка трафика для защиты от нелегальных операций.

4. User Plane Function (UPF) – Шифрование и контроль целостности данных пользователя. Диагностика и отчетность о состоянии трафика, позволяющая обнаружить отклонения и угрозы. Маршрутизация и передача данных с соблюдением требований безопасности и качества обслуживания (QoS).

5. Access Management Function (AMF) – Координация и управление доступом пользователей к сетям. Генерация и обработка секретных ключей, необходимых для защиты коммуникаций. Реализация механизма Secure Anchor Function (SEAF) для усиления защиты данных.

6. Service Communication Proxy (SEPP) – Защита сигнального трафика между сетями разных операторов, включая deep packet inspection

(DPI) и шифрование. Прокси-сервер для фильтрации и блокировки опасных или нежелательных соединений.

7. Session Management Function (SMF) – Управление сессиями, поддержание стабильности соединений и безопасности транзакций. Назначение и изменение параметров безопасности для сессий. Связывание правил политики Quality of Service (QoS) с управлением сеансами.

8. Policy Control Function (PCF) – Установка и соблюдение правил безопасности, связанных с качеством обслуживания и доступом к услугам. Принятие решений относительно распределения сетевых ресурсов и соответствия пользовательскому поведению.

9. Application Function (AF) – Организация и защита сервисов приложений, используемых в сетях 5G. Менеджмент данных и политик безопасности, определяющих условия предоставления услуг.

10. Network Slice Selection Function (NSSF) – Безопасность выделения и управления сетевыми срезами (slices), предназначенных для конкретных бизнес-процессов и приложений. Установление политики безопасности для определенных сегментов сети.

11. Non-3GPP Interworking Function (N3IWF) – Интеграция с сетями Wi-Fi, Ethernet и другими технологиями для расширения покрытия сети 5G. Осуществление проверок безопасности для установления безопасных соединений с ненадежными сетями.

12. Authentication Server Function (AUSF) – Ответственность за процессы аутентификации и верификацию подлинности пользователей. Работа совместно с базой данных подписчиков (UDM) для хранения и управления профилями пользователей.

13. Unified Data Management (UDM) – управления пользовательскими данными и политиками безопасности. Генерация учетных данных для аутентификации и управление регистрационными действиями.

14. Charging Function (CHF) – Администрирование и защита процесса начисления оплаты за сетевые ресурсы и услуги. Сбор данных о потребляемых услугах и их тарификация с контролем целостности данных.

15. Network Exposure Function (NEF) – Обеспечение внешнего доступа к функциональности сети 5G с соблюдением высоких стандартов безопасности. Применение авторизации и аутентификации для ограничения доступа посторонних приложений и сервисов.

Понимание архитектуры 5G и функционала ее компонентов позволяет выявить потенциальные цели атак злоумышленников – сервисы, ответственные за биллинг, управление базами данных, политики и доступ к системе. Элементы, взаимодействующие с внешними сетями, такие как NR/gNB, NEF, N3IWF, SEPP, UPF и AMF, являются наиболее уязвимыми и станут первоочередными целями для атак. Возможные угрозы для сетей 5G, представлены на рисунке 2 [5].

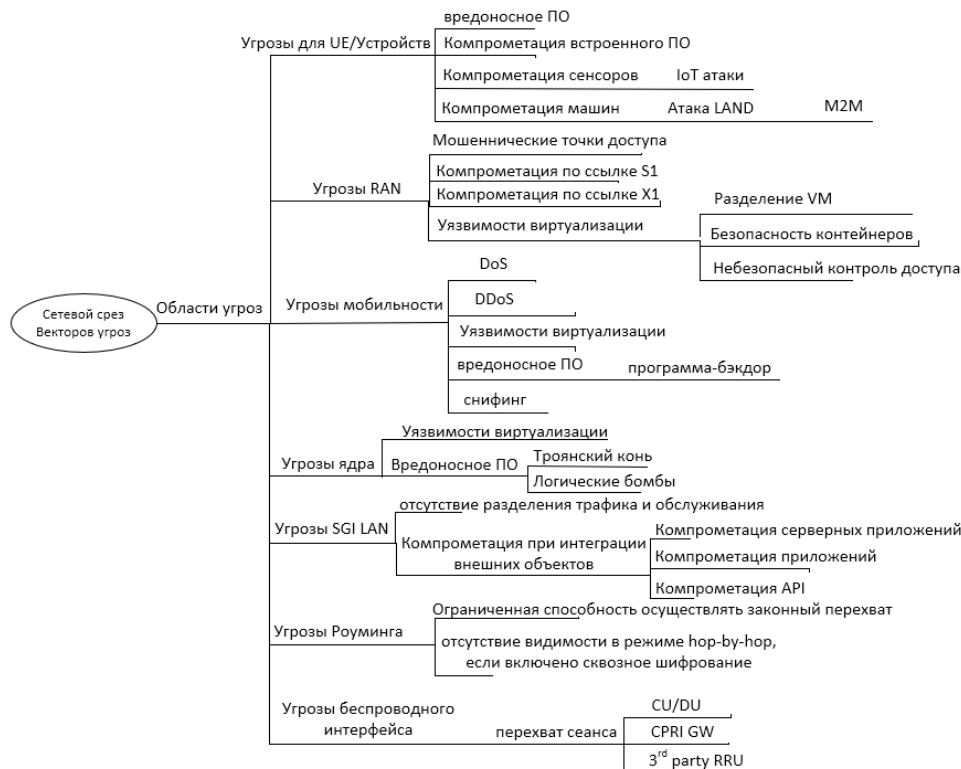


Рис. 2. Обзор векторов угроз 5G

Рассмотрим некоторые угрозы для сетей.

1. Угрозы безопасности пользовательского оборудования (UE): Заражение устройства вредоносным ПО, ведущее к компрометации данных и самого устройства. Несанкционированный доступ к конфиденциальной информации, хранящейся на устройстве. Возможность использования устройства в качестве узла ботнета для организации атак типа DoS/DDoS.

Меры митигации: Внедрение средств анализа состояния UE для раннего выявления вредоносного ПО и мониторинга трафика. Развитие механизмов контроля соблюдения стандартов информационной безопасности (ИБ). Регулярный аудит и модернизация механизмов защиты.

2. Угрозы через беспроводной интерфейс (Air Interface): Атаки типа "Человек посередине" (Man-in-the-Middle), позволяющие злоумышленникам перехватывать и изменять данные. Взлом и искажение пилотов сигнала, влияющих на работу массовых массивов антенн (Massive MIMO) и технологию beamforming. Утечка данных из-за недостатка шифрования или неправильной конфигурации безопасности.

Меры митигации: Использование надежных механизмов шифрования для передачи данных. Повышение уровня аутентификации и авторизации для доступа к базовой станции (gNB). Постоянный мониторинг логов и быстрое реагирование на инциденты.

3. Угрозы базовой сети (Core Network, CN): Незаконный доступ к виртуальным машинам и контейнерам, работающим в составе сети 5G. Эксплуатация уязвимостей в программах управления сетью (микросервисы, оркестраторы). Распространение вредоносных данных через защищенные каналы между компонентами сети.

Меры митигации: Переход на более надежные альтернативы протоколам SS7 и Diameter. Улучшенная защита микросервисов (контроллер идентификации и доступа, контроль целостности и прозрачность контейнеров).

4. Угрозы серверов приложений: Нарушение работы серверов приложений, находящихся вне инфраструктуры 5G, путем взлома или перегрузки (DDoS-атаки). Использование открытых программных решений (open source), содержащих уязвимости, что ведет к риску компрометации инфраструктуры. Отсутствие достаточной изоляции серверов приложений от остальной сети.

Меры митигации: Увеличение уровня шифрования и использование обновленных стандартов (NEA0, 128-NEA1, 128-NEA2). Следование рекомендациям стандарта 3GPP по обеспечению безопасности и конфиденциальности

5. Угрозы от использования open-source решений: Наличие уязвимостей в открытом коде, ставящем под угрозу безопасность сети. Медленная реакция на появление и устранение багов и эксплойтов. Доступ злоумышленников к чувствительным данным, хранимым в open-source проектах.

Меры митигации: Закрепление внутренних процедур безопасной разработки ПО. Периодическое тестирование на наличие уязвимостей (пен-тесты). Модернизация процедур оперативного исправления найденных недостатков

6. Угрозы искусственного интеллекта (AI) и машинного обучения (ML): Манипуляция моделями машинного обучения (например, отравления данных, spoofing, backdoor attacks). Неправильная интерпретация данных, ведущая к ошибочным действиям систем защиты. Этические и правовые вопросы, связанные с обработкой персональных данных и правом собственности на данные.

Меры митигации: Регулярный мониторинг и аудит моделей машинного обучения. Четко регулируемый доступ к модулям AI и ML. Разработка единого международного стандарта для безопасного использования ИИ.

7. Физические угрозы: Физические повреждения или вмешательство в инфраструктуру сети (антенны, центры обработки данных). Воздействие электромагнитных полей, способных вызвать отказ оборудования. Потеря данных или ухудшение качества обслуживания из-за физической деструкции.

Меры митигации: Шифрование и защита данных на физическом уровне (PLS). Сокращение мощности передач для усложнения атаки. Применение расширяющих методов передачи сигнала (DSSS/FHSS).

8. Государственные требования и надзор. Необходимость реализации законного перехвата данных ставит сети под риск, так как полного запрета старых протоколов связи (4G/LTE) достичь нельзя.

Меры митигации: Внедрение аналитических систем с поддержкой машинного обучения и искусственного интеллекта для своевременного выявления аномального поведения. Баланс между законным требованием государственных органов и интересами конфиденциальности пользователей

9. Проблемы взаимодействия с уязвимыми сетями LTE: Необходимость поддерживать обратную совместимость с менее защищенными сетями предыдущего поколения (4G/LTE), оставляющими лазейки для атак. Недостаточность встроенных мер безопасности при взаимодействии двух типов сетей.

Меры митигации: Реализация принципа "нулевого доверия" (Zero Trust) для усиления защиты взаимодействия между сетями. Упрощение перехода на более безопасные и современные технологии.

10. Программно-определяемая сеть (SDN). Возможность атаки на контроллеры SDN, управляющего основной частью инфраструктуры сети. Утрата изолированности отдельных сегментов сети и распространение атак на всю инфраструктуру. Недостаточно надежная аутентификация и шифрование данных внутри самой SDN-инфраструктуры.

Меры митигации: Усиленная аутентификация и контроль доступа к SDN-ресурсам. Междоменная изоляция сегментов сети и установление правил взаимодействия между ними.

Теперь проведем оценку рисков и оценку предложенных мер, по смягчению риска. Для оценки степени риска была использована технология CASE (Consequence, Assets, Source, Event) [6]. Использовать будем матрицу оценки рисков размерностью 5x5, которая представлена на рис.3.

	Низкая вероятность (L)	Средняя вероятность (M)	Высокая вероятность (H)	Очень высокая вероятность (Vh)	Критическая вероятность (C)	где	
Критическое воздействие (C)	4	5	5	5	5	Критический (C)	5
Очень высокое воздействие (Vh)	3	4	4	4	5	Очень высокий (VH)	4
Высокое воздействие (H)	2	3	3	4	5	Высокий (H)	3
Среднее воздействие (M)	1	2	2	3	4	Средний (M)	2
Незначительное воздействие (L)	1	1	2	2	3	Низкий (L)	1

Рис. 3. Матрица оценки рисков (составлено авторами)

В таблице 1 представлена оценка рисков реализации угроз До и После принятия мер по их снижению. Вероятность наступления угрозы (Probability) классифицируется так: Низкая (0-20%), Средняя (21-40%), Высокая (41-60%), Очень высокая (61-80%) и Критическая (81-99%).

Таблица 1.

Оценка риска реализации угрозы До и После применения мер

Threat (Th)	ДО			ПОСЛЕ		
	Impact	Prob	R.Lev	Impact	Prob	R.Lev
Th1: Угрозы безопасности UE	H	H	3	M	M	2
Th2: Угрозы безопасности через беспроводной интерфейс	M	H	2	L	L	1
Th3: Угрозы безопасности в CN	C	H	5	H	M	3
Th4: Угрозы безопасности сервера приложений	Vh	H	4	M	M	2
Th5: Использование open-source ПО	H	H	3	M	L	1
Th6: Угрозы безопасности AI и ML	Vh	M	4	M	M	2
Th7: Угрозы безопасности на физическом уровне	H	M	3	M	M	2
Th8: Требования государства	H	M	3	M	L	1
Th9: Угрозы взаимодействия с сетью LTE	VH	H	4	M	M	2
Th10: Угрозы безопасности SDN	H	H	3	M	M	2

Проведем расчеты на основе данных из таблицы 2.

$$Probability_{lev} = \frac{\sum_{i=1}^{10} (Thl_{aft} - Thl_{bef})}{10} = 20\% \quad (1)$$

$$Impact_{lev} = \frac{\sum_{i=1}^{10} (Thl_{aft} - Thl_{bef})}{100\%} = 28\% \quad (2)$$

где, $Th[i]_{aft}$ – угроза После. $Th[i]_{bef}$ – угроза До.

Проведенные расчеты показывают, что предложенные меры существенно повысят безопасность сетей 5G. В среднем вероятность реализации угрозы снижается на 20%, а уровень её воздействия — на 28%. Графическое представление результатов расчетов, показанное на рисунке 4, наглядно подтверждает этот вывод.



Рис.4. Результаты оценки (а) уровня воздействия, (б) уровня вероятности (с) уровня риска реализации угрозы ДО и ПОСЛЕ реализации мер по снижению воздействия (разработано авторами)

Заключение

В настоящей работе проведен анализ рисков информационной безопасности в сетях 5G и предложены меры по их минимизации. Изучив структуру и функциональность архитектуры сети 5G, был выявлен целый ряд

угроз, затрагивающих все компоненты сети. Было установлено, что внедрение сетей 5G сопровождается рядом серьёзных вызовов, таких как высокие требования к конфиденциальности и целостности данных, проблемы совместимости с существующими сетями прошлых поколений (4G/LTE), а также растущие риски, связанные с интеграцией искусственного интеллекта и машинного обучения. Особое внимание уделено ряду факторов, оказывающих существенное влияние на уровень безопасности:

- Совершенствование методов шифрования и аутентификации;
- Оптимизация процессов мониторинга и анализа сетевого трафика;
- Минимизация зависимостей от устаревших технологий и принятие согласованных международных стандартов безопасности.

Предлагаемые меры позволили значительно сократить вероятность реализации угроз и минимизировать их негативное воздействие. Приведенные расчёты показывают, что вероятность реализации угроз снизилась примерно на 20%, а уровень их воздействия уменьшился почти на треть (28%). Такой эффект достигается за счёт комплексного подхода, объединяющего техническую экспертизу, аналитику и внедрение современных стандартов безопасности.

Проведенное автором исследование подчеркивает актуальность и необходимость дальнейшей работы в направлении повышения безопасности сетей 5G.

Библиографический список:

1. Ahmad, Ijaz & Suomalainen, Jani & Huusko, Jyrki. (2019). 5G-Core Network Security. In book: Wiley 5G Ref (pp.1-18). DOI:10.1002/9781119471509.w5GRef151.
2. X. Zhang, J. Fei, H. Jiang and X. Huang, "Research on Power 5G Business Security Architecture and Protection Technologies," 2021 6th International Conference on Power and Renewable Energy (ICPRE), Shanghai, China, 2021, pp. 913-917, doi: 10.1109/ICPRE52634.2021.9635437
3. 5G Americas (2020). The Status of Open Source for 5G. 5G Americas White Paper. <https://www.5gamericas.org/the-status-of-open-source-for-5g/>
- 4 3rd Generation Partnership Project; Technical specification Group Radio Access Network; Study on New Radio Access Technology: Radio Access Architecture and Interfaces // 3GPP TR 38.801 Technical Report (2017-03) Retrieved from https://panel.castle.cloud/view_spec/38801-e00/pdf/
5. 5G Americas. (2020, April 27). The evolution of security in 5G. A “Slice” of Mobile Threats. 5G Americas White Paper. <https://www.5gamericas.org/the-evolution-of-security-in-5g-2/>
6. Talbot, J. (2023, October 4). What’s right with risk matrices? juliantalbot. <https://www.juliantalbot.com/post/2018/07/31/whats-right-with-risk-matrices>