Иванов Денис Алексеевич,
Филиал Военного учебно-научного центра
Военно-воздушных сил «Военно-воздушная академия»
в г. Челябинске (филиал ВУНЦ ВВС «ВВА»),
Челябинск, Россия
D. A. Ivanov,
Branch of the Military Educational and
Scientific Center of the Air Force "Air Force Academy"
in Chelyabinsk (Branch of the Military Educational and
Scientific Center of the Air Force "VVA"), Chelyabinsk, Russia

Попов Юрий Леонидович,
Филиал Военного учебно-научного центра
Военно-воздушных сил «Военно-воздушная академия»
в г. Челябинске (филиал ВУНЦ ВВС «ВВА»),
Челябинск, Россия
Y. L. Popov,
Branch of the Military Educational and
Scientific Center of the Air Force "Air Force Academy"
in Chelyabinsk (Branch of the Military Educational and
Scientific Center of the Air Force "VVA"), Chelyabinsk, Russia

Крутеленок Михаил Андреевич,
Филиал Военного учебно-научного центра
Военно-воздушных сил «Военно-воздушная академия»
в г. Челябинске (филиал ВУНЦ ВВС «ВВА»),
Челябинск, Россия
M.A. Krutelenok,
Branch of the Military Educational and
Scientific Center of the Air Force "Air Force Academy"
in Chelyabinsk (Branch of the Military Educational and
Scientific Center of the Air Force "VVA"), Chelyabinsk, Russia

СЕТИ 5G: ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ
APPLICATION OF SUPERCONDUCTING QUANTUM INTERFERENCE DEVICES IN MARINE NAVIGATION

Аннотация: Сети пятого поколения (5G) представляют собой значительный шаг вперед в области мобильной связи, обеспечивая высокую скорость передачи данных, низкую задержку и возможность подключения множества устройств. Однако с внедрением 5G возникают новые вызовы в области конфиденциальности и безопасности. В данной статье рассматриваются ключевые аспекты обеспечения безопасности сетей 5G, включая угрозы, связанные с уязвимостями инфраструктуры, а также методы защиты данных пользователей. Особое внимание уделяется вопросам шифрования, аутентификации и управления доступом, а также законодательным и нормативным инициативам, направленным на защиту конфиденциальности пользователей. В заключение подчеркивается необходимость комплексного подхода к обеспечению безопасности в условиях быстро развивающейся технологической среды.

Abstract: Fifth-generation (5G) networks represent a significant advancement in mobile communication, providing high data transfer speeds, low latency, and the ability to connect numerous devices. However, the implementation of 5G brings new challenges in the areas of privacy and security. This article examines the key aspects of ensuring the security of 5G networks, including threats related to infrastructure vulnerabilities and methods for protecting user data. Special attention is given to issues of encryption, authentication, and access control, as well as legislative and regulatory initiatives aimed at safeguarding user privacy. In conclusion, the necessity of a comprehensive approach to security in a rapidly evolving technological environment is emphasized.

Ключевые слова: 5G, безопасность, конфиденциальность, мобильные сети, шифрование, аутентификация, управление доступом, уязвимости, защита данных, законодательство, киберугрозы, инфраструктура, стандарты безопасности, приватность пользователей, технологии связи.

Keywords: 5G, security, privacy, mobile networks, encryption, authentication, access control, vulnerabilities, data protection, legislation, cyber threats, infrastructure, security standards, user privacy, communication technologies.

Основные составляющие телекоммуникационной инфраструктуры и обеспечение безопасности на сетях 5G.

Современная телекоммуникационная сеть состоит из четырех основных логических сетевых составляющих, а именно: сети фиксированного и радиодоступа, опорной сети, транспортной сети и межсетевой сети [5].

1. Сеть фиксированного и радиодоступа.

Существует много типов сетей доступа, таких как сети радиодоступа 3GPP (RAN), включая GSM/GPRS, UMTS, EUTRAN, NG-RAN (5G), а также спутниковые и не-3GPP сети доступа, сети беспроводного доступа Wi-Fi или фиксированная (проводная) сеть доступа. Open RAN – это архитектура открытой сети радиодоступа (RAN), стандартизированная O-RAN Alliance на основе 3GPP и других стандартов.

2. Опорная сеть может предоставлять ряд услуг абонентам, которые подключены через сеть доступа к опорной сети (ядру/Core), например, телефонные звонки и соединения для передачи данных. Пользовательские устройства, такие как мобильные телефоны, могут оставаться на связи независимо от времени и места, что возможно благодаря стандартизированным системам сигнализации и интерфейсам.

3. Транспортная сеть поддерживает связь сети доступа (например, RAN) с опорной сетью (ядром/Core), причем и базовые станции в сети радиодоступа связаны друг с другом поверх транспортной сети.

4. Сеть межсоединений соединяет опорные уровни (ядра/Core) различных сетей друг с другом

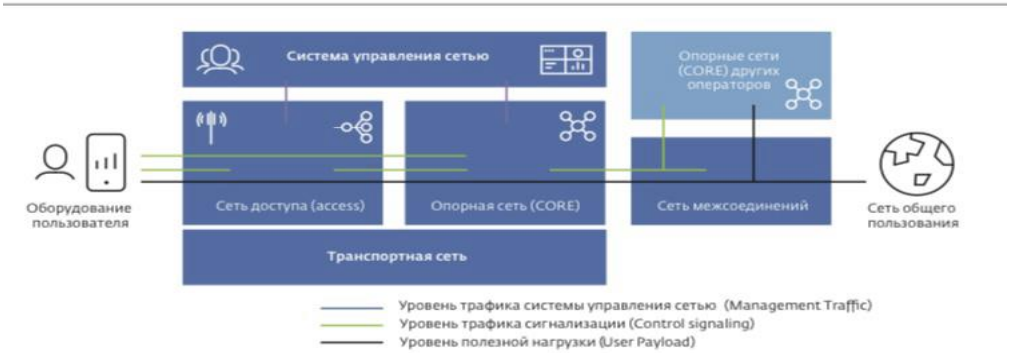

Рис.1. Логические элементы и плоскости системы безопасности сети 5G

Сети электросвязи по всему миру передают голос и данные с высоким качеством и уровнем согласованности. Каждой из перечисленных выше четырех составляющих телекоммуникационной инфраструктуры соответствуют три плоскости, отвечающие за перенос различных типов трафика. Каждая из указанных ниже плоскостей может подвергаться уникальным типам угроз. Также существуют единые угрозы, которые могут повлиять на все три плоскости одновременно:

• плоскость сигналов сигнализации (Control Plane, C-plane, CP), которая передает трафик сигнализации.

Сигнализация – это метаданные, поддерживающие сети, включая получение такой информации, как, например, географическое положение абонента.

Может быть предпринята попытка модификации сигнального трафика для перенаправления вызовов или перехвата SMS-сообщений с целью подслушивания или отказа в обслуживании. Сегодняшние риски безопасности намного более развиты и сложны по сравнению с технологиями предыдущего поколения. При разработке сигнализации предыдущих поколений, например 2G, безопасности уделялось меньше внимания. Частично это было обусловлено высоким уровнем доверия к сигнальным узлам. Теперь известно, что телекоммуникационная сигнализация регулярно подвергается атакам. В текущей стандартизации SG 3GPP безопасность играет центральную роль;

○ плоскость пользователя (User Plane, U-plane,UP), которая передает полезную нагрузку, то есть реальный клиентский трафик. Трафик полезной нагрузки пользователя содержит фактические данные, которые передаются пользователю. Без надлежащих мербезопасности конфиденциальность пользователя и конфиденциальность корпоративных или государственных данных окажутся под угрозой;

○ плоскость управления (Management Plane, M-plane, MP), которая передает административный трафик контроля и управления сетью.

○ Уровень управления необходим для обеспечения оптимального функционирования бизнеса поставщика услуг. Этот уровень привлекателен для хакеров, поскольку они могут получить доступ к сетевым ресурсам, где можно манипулировать сетевым трафиком и данными, нарушать их работу. Снижение рисков и угроз, связанных с управлением сетью, требует внедрения политик безопасности и нескольких мер безопасности, таких как контроль доступа и мониторинг безопасности.

Логические элементы и плоскости системы безопасности сети SG представлены на рис.1.

Сегментированная архитектура сети 5G представлена на рис.2, а наиболее значимые угрозы для каждого из главных компонентов сети SG – в табл.1.

Рис.2. Сегментированная архитектура 5G-сети, используемая для описания угроз безопасности

Функциональное разделение сети радиодоступа RAN, представленное в документах O-RAN Alliance, основано на следующих ключевых принципах:

- разделение аппаратного и программного обе-
- облачная инфраструктура;
- стандартизированные и открытые интерфейсы между сетевыми функциями.

O-RAN Alliance определил открытую и безопасную архитектуру, которая включает безопасные интерфейсы между всеми ее компонентами. Обмен данными по этим интерфейсам криптографически защищен шифрованием, приняты меры для защиты целостности и защиты от воспроизведения.

Базирующаяся в США компания Altiostar предоставляет, например, программное обеспечение для открытой платформы виртуализированного радиодоступа (Open VRAN) 4G и 5G, которое поддерживает открытые интерфейсы и предусматривает виртуализацию модуля электронной обработки базовой станции (Baseband Unit, BBU) для построения дезагрегированной, мультивендорной, масштабируемой и ориентированной на облачные решения мобильной связи.

На рис.3. представлена безопасная архитектура O-RAN в соответствии с документом "Безопасность в Open RAN", подготовленным компанией Altiostar [6].Показана плоскость передачи сигналов управления и пользовательских данных (CUS-plane), необходимых для синхронизации действий между несколькими устройствами радиодоступа, а также плоскость управления (M-plane), реализованная поверх протоколов SSH/TLS таким образом, радиоблоком Open Radio Unit (O-RU) осуществляется от блока Open Distributed Unit (O-DU) и/или 44

ПЕРВАЯ МИЛЯ

от централизованной системы управления сетью Network Management System (NMS) с использованием интерфейса NETCONF.

В документах O-RAN Alliance определены две модельные конфигурации M-plane для управления радиоблоком O-RU (отражены на рис.4 как O-RAN,Hybrid M-plane over SSH/TLS и O-RAN Hierarchical,M-plane over SSH/TLS):

• иерархическая модель (Hierarchical M-plane): управляется от O-DU. O-DU принимает сигналы монито-ринга/управления от подключенного к нему O-RU, что освобождает NMS от мониторинга/управления всеми радиоблоками O-RU. Если существующая NMS не поддерживает открытый интерфейс NETCONF, модель позволяет построить сеть, не затрагивая систему NMS. В этой модели O-DU выпол-няет функцию клиента NETCONF.

• гибридная модель (Hybrid M-plane): в этой конфигурации O-RU управляется не только ОТ O-DU, но и от NMS. Преимущество модели состоит в том, ЧТо NMS может отслеживать/ управлять и другими сетевыми устройствами, обеспечивая единообразное обслуживание, мониторинг и управление всеми O-DU. В этой модели NMS выполняет функцию клиента NETCONE, а O-RU – сервера NETCONF.

Сокращения и обозначения на рис.3:

• PDCP (Packet Data Convergence Protocol): протокол обрабатывает RRC-сообщения в плоскости управления (control plane) и IP-пакеты в пользовательской плоскости (user plane) в системах 4G/LTE. Применяется на участке eNodeB

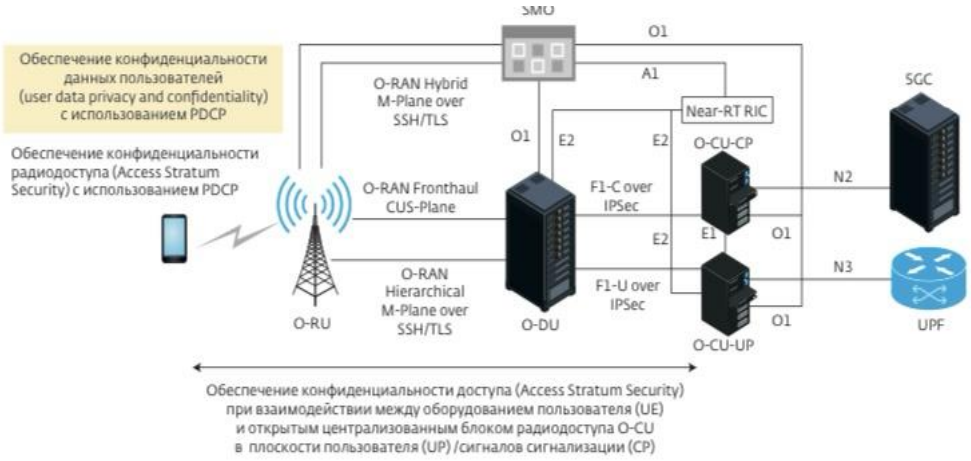

Рис.3. Безопасная архитектура O-RAN

(базовая станция) – UE (оборудование пользователя). PDCP предусматривает шифрование данных (как пользовательских, так и управляющих), обеспечивает их целостность (только для управляющих данных);

o RRC (Radio Resource Control) – протокол RRC используется для передачи общей информации, которая касается всех UE, и специальной, относящейся только к определенным UE. Для передачи системной информации используются три типа RRC-сообщений: MIB, SIBl и сообщения системной информации (System Information, SI);

o IPSec (IP Security): набор протоколов для обеспечения защиты данных, передаваемых межсетевому протоколу IP. Позволяет подтверждать подлинность (аутентифика-цию), проверять целостность и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищенного обмена ключами в сети Интернет. В основном применяется для организации VPN-соединений;

o PDU (protocol data unit): обобщенное название фрагмента данных на разных уровнях модели OSI: кадр Ethernet, IP-пакет, UDP-датаграмма, TCP-сегмент и т. д.;

o 5GC: опорная (Core) сеть 5G;

o UPF (User Plane Function): одна из сетевых функций (Network Functions, NF) уровня ядра (Core) сети 5G (SCC). UPF отвечает за маршрутиза-цию и пересылку пакетов, проверку пакетов, обработку QoS и внешний сеанс PDU для соединения сети передачи данных (DN) в архитектуре SG;

o DU (Destributed Unit): распределенный блок, часть функциональности BBU;

o CU (Centrlized Unit): централизованный блок, часть функциональности BBU;

o SMO (Service Management and Orchestration system): система управления и оркестрации при предоставлении услуг/сервисов;

o M-plane (Management plane): уровень управления сетью – соединение между открытым радиоблоком O-RU и открытым распределенным блоком O-DU;

o CUS-plane (Control user synchronization plane): уровень синхронизации – многофункциональный интерфейс используется для передачи сигналов управления и пользовательских данных соответственно, обеспечивает синхрони-зацию действий между несколькими устройствами радиодоступа;

o TLS (Transport Layer Security): протокол защиты транспортного уровня, стандартный протокол, который используется для создания защищенных онлайн-соединений;

Таблица 1.

Наиболее значимые угрозы для основных компонентов сети 5G

Угрозы для RAN	Угрозы для опорной сети и сервисов оператора	Угрозы для MEC	Угрозы для инфраструктуры сети 5G из внешних сетей
DDoS-атаки от оконечных устройств	Программные и аппаратные сбои элементов ядра сети, ошибки конфигурации	Физический доступ нарушителя к оборудованию	DDoS-атаки из Интернета
Внедрение поддельных базовых станций	Внедрение вредоносного кода или использование уязвимостей компонентов инфраструктуры	Поддельное или уязвимое стороннее приложение в экосистеме	Несанкционированный доступ к API поставщиков сервисов
Атаки на беспроводные интерфейсы – перехват, подмена пользовательских данных	Нарушение изоляции сегментов, несанкционированный доступ к сегменту сети	Проникновение в корпоративные или операторские сети из узлов MEC	Несанкционированный доступ к интерфейсу управления из внешних сетей

• SSH (Secure Shellhttps://ru.wikipedia.org/wiki/SSH – cite_note-1): безопасная оболочка – сетевой протокол прикладного уровня, позволяющий обеспечить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов);

• F1-C (Fl Application Protocol, FIAP, control plan):прикладной интерфейс / протокол F1AP в соответствии с 3GPP TS 38,473 version 15.3.0 Release 15. В примере на рис.4 передается поверх протокола IPsec;

• FI-U (Fl Application Protocol, FIAP, user plan): прикладной интерфейс / протокол FlAP (Fl Application Protocol, FIAP) в соответствии с 3GPP TS 38.473 version 15.3.0 Release 15, В примере на рис.4 передается поверх протокола IPsec.

В табл. 1 представлены наиболее значимые угрозы для основных компонентов сети SG.

Сокращения и обозначения в табл.1:

• DoS (Denial of Service, отказ в обслуживании): хакерская атака на вычислительную систему с целью довести ее до отказа, то есть создание условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам) либо доступ будет затруднен. Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (Distributed Denial of Service, распределенная атака типа "отказ в обслуживании"). Проводится, когда требуется вызвать отказ в обслуживании хорошо защищенной крупной компании или правительственной организации.

Злоумышленник отправляет запросы из нескольких взломанных систем. Конечная цель – вывод из строя систем компании и прерывание ее бизнес-процессов. В защищенной сети (например, по рекомендации специалистов Kaspersky) с началом атаки весь трафик перенаправляется в центры очистки, которые распознают и удаляют "мусорный" трафик, пропуская на защищаемый ресурс только трафик от легитимных пользователей в соответствии с выбранной схемой подключения;

○ MEC (Multi-access Edge Computing): этот функционал дает возможность разработчикам приложений и поставщикам контента использовать на периферии сети преимущества облачных вычислений и среды ИТ-услуг. Преимущества решения – обеспечение сверхмалой задержки и высокой пропускной спо-собности, а также доступа в реальном времени к информации радиосети, которая может быть использована для приложений;

○ API (Application Program Interface): программный интерфейс приложения (интерфейс прикладного программирования), включающий описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой.

Вопросы безопасности должны приниматься во внимание на всех этапах создания, эксплуатации и развития телекоммуникационной сети, включая:

сетевой дизайн (Network design). Поставщики сетей при проектировании, разработке и построении инфраструктуры используют согласованные международные стандарты для функциональных сетевых элементов и систем, которые играют решающую роль в обеспечении функциональности и безопасности конечного сетевого продукта;

• конфигурация сети (Network configuration).

На этапе развертывания сети настраиваются на достижение целевого уровня безопасности как ключевого фактора для установки параметров безопасности, укрепления безопасности и отказоустойчивости сети. Проектирование и разработка, выполняемые поставщиком сети, – важная часть обеспечения функциональности и безопасности конечного сетевого продукта;

• развертывание и эксплуатация сети (Network deployment and operation). Операционные процессы должны гарантировать заданные уровни безопасности. На этапе развертывания сети обеспечивается установка исходных параметров ее безопасности, закладываются основы повышения устойчивости сетевой инфраструктуры к несанкционированным действиям.

Операционные процессы должны упрощать работу сети и обеспечивать заданный уровень безопасности на всех этапах ее эксплуатации и развития.

ЗАКЛЮЧЕНИЕ

Сети 5G открывают новые горизонты для мобильной связи и цифровых технологий, предлагая беспрецедентные возможности для повышения скорости передачи данных и подключения множества устройств. Однако с этими преимуществами приходят и серьезные вызовы в области конфиденциальности и безопасности. Уязвимости в инфраструктуре, потенциальные киберугрозы и необходимость защиты личных данных пользователей требуют комплексного подхода к обеспечению безопасности. Для эффективного решения этих проблем необходимо внедрение современных методов шифрования, надежной аутентификации и строгого управления доступом. Также важным аспектом является разработка и соблюдение законодательных и нормативных инициатив, направленных на защиту прав пользователей и обеспечение их конфиденциальности. В условиях стремительного развития технологий и увеличения числа подключенных устройств, обеспечение безопасности сетей 5G должно стать приоритетом для всех участников – от операторов связи до разработчиков программного обеспечения и государственных органов. Только совместными усилиями можно создать безопасную и надежную экосистему, которая позволит максимально использовать потенциал 5G, минимизируя риски для пользователей и общества в целом.

Список литературы:

1. Журнал "Открытые Системы. СУБД". Безопас-ность SG. (Электронный ресурс). URL: https:// www.osp.ru/os/2020/02/13055462/

2. Рекомендация Международного союза электро-связи МСЭ-Т E.408 Telecommunication networks security requirements (05/2004) (Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors Network management – International network management).

3. Рекомендация Международного союза электро-связи МСЭ X.805 Security architecture for systems providing end-to-end communications (10/2003) (Se-ries X: Data Networks and Open System Communi-cations. Security).

4. Рекомендация Международного союза электро-связи МСЭ M.3016.1 Security for the management plane: Security requirements (04/2005) (Series M: Telecommunication Management, Including TMN and Network Maintenance Telecommunications management).

5. A guide to 5G network security. Conceptualizing security in mobile communication networks – how does 5G fit in?. WP. Ericsson. (Электронный ресурс), https://www.ericsson.com/en/security/a- guide-to-5g-network-security.

6. WP Security in Open RAN, Altiostar. (Электронный ресурс). URL: https://www.altiostar.com/white-pa-per-security-in-open-ran/ 2021.

7. Как обеспечить безопасность сетей SG. Cnews. (Электронный ресурс). URL: https://safe.cnews. ru/articles/2020-11-20_kakie_ugrozy_bezopasnosti_nesut

References:

1. Journal "Open Systems. DBMS". Security of SG. (Electronic resource). URL: https://www.osp.ru/os/2020/02/13055462/ (accessed: 08.10.2021).

2. Recommendation ITU-T E.408 Telecommunication networks security requirements (05/2004) (Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors Network management – International network management).

3. Recommendation ITU-T X.805 Security architecture for systems providing end-to-end communications (10/2003) (Series X: Data Networks and Open System Communications. Security).

4. Recommendation ITU-T M.3016.1 Security for the management plane: Security requirements (04/2005) (Series M: Telecommunication Management, Including TMN and Network Maintenance Telecommunications management).

5. A guide to 5G network security. Conceptualizing security in mobile communication networks – how does 5G fit in? WP. Ericsson. (Electronic resource), https://www.ericsson.com/en/security/a-guide-to-5g-network-security.

6. WP Security in Open RAN, Altiostar. (Electronic resource). URL: https://www.altiostar.com/white-paper-security-in-open-ran/ 2021.

7. How to ensure the security of SG networks. Cnews. **(**Electronic resource). URL: https://safe.cnews.ru/articles/2020-11-20_kakie_ugrozy_bezopasnosti_nesut/.