СЕТИ 5G: обеспечение конфиденциальности и безопасности

Часть 2

С.Коган, к.т.н., советник генерального директора компании "Т8" по формированию технической стратегии / kogan@t8.ru

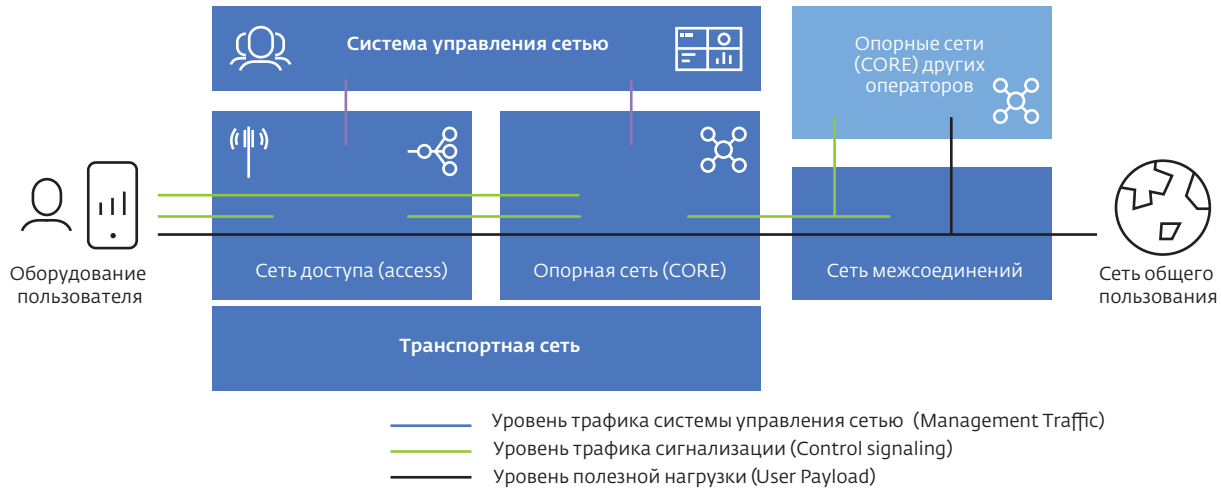
УДК 004.056.53, DOI: 10.22184/2070-8963.2021.100.8.42.47

Современные операторы сетей, поставщики контента и услуг должны соблюдать требования безопасности, которыми регулируются управление и защита конфиденциальных данных от раскрытия, кражи и неправомерного использования. Количество конфиденциальных данных, генерируемых компаниями и частными пользователями, неуклонно растет. Традиционно хранящиеся и обрабатываемые на месте данные в настоящее время транспортируются через общие сетевые ресурсы, зачастую через глобальную сеть. Широкое использование виртуальных объектов и облачных сетей создает новые угрозы уязвимости сети к внешним атакам. Безопасность – одно из важнейших преимуществ 5G, которые будут служить критически важной инфраструктурой для оцифровки, автоматизации и подключения к машинам, роботам, управлению транспортными средствами и т. п. В статье рассмотрены вопросы обеспечения безопасности и защиты конфиденциальных данных при оказании телекоммуникационных услуг на базе сетей 5G. Во второй части материала основное внимание уделено решению задач безопасности на сетях мобильной связи следующего поколения.

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.



Источник: A guide to 5G network security. Conceptualizing security in mobile communication networks – how does 5G fit in?. WP Ericsson, 2018; https://www.ericsson.com/en/security/a-guide-to-5g-network-security

Рис.2. 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 5G 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 мер безопасности 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 5G представлены на рис.2 [5].

Сегментированная архитектура сети 5G представлена на рис.3, а наиболее значимые угрозы для каждого из главных компонентов сети 5G – в табл.2 [7].

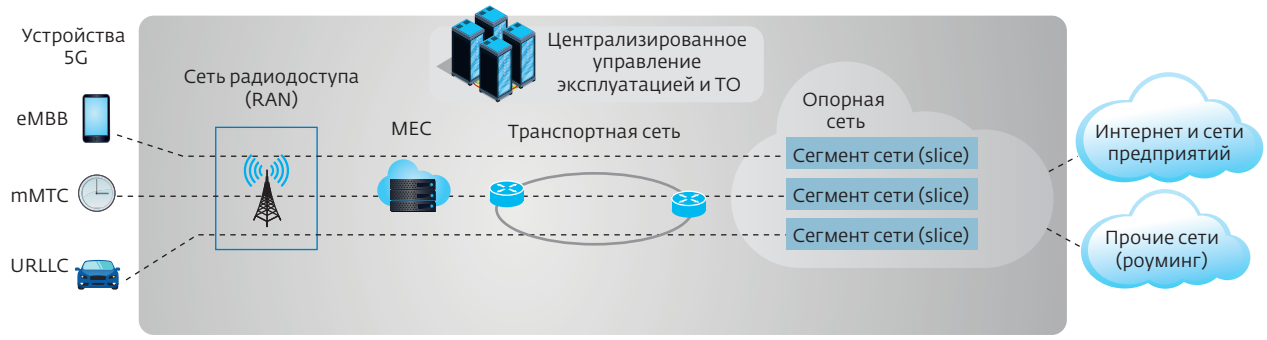


Рис.3. Сегментированная архитектура 5G-сети, используемая для описания угроз безопасности

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

- разделение аппаратного и программного обеспечения;
- 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.

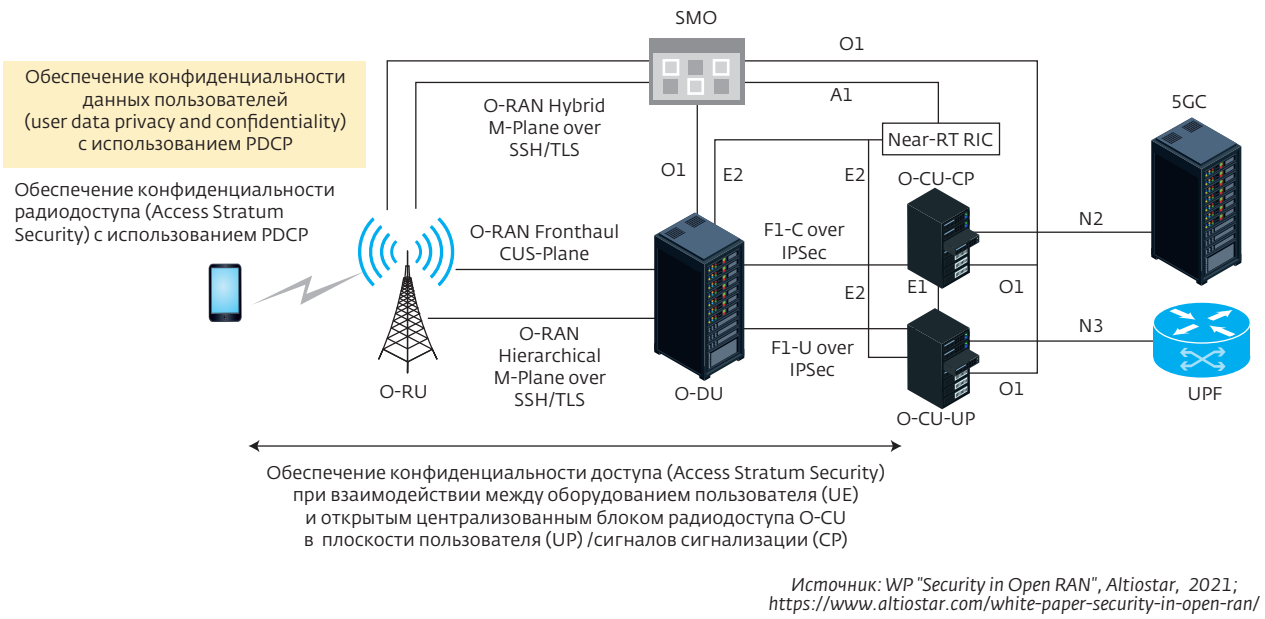
На рис.4 представлена безопасная архитектура O-RAN в соответствии с документом "Безопасность в Open RAN", подготовленным компанией Altiostar [6]. Показана плоскость передачи сигналов управления и пользовательских данных (CUS-plane), необходимых для синхронизации действий между несколькими устройствами радиодоступа, а также плоскость управления (M-plane), реализованная поверх протоколов SSH/TLS таким образом, что управление радиоблоком Open Radio Unit (O-RU) осуществляется от блока Open Distributed Unit (O-DU) и/или 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): в этой конфигурации O-RU управляется от O-DU. O-DU принимает сигналы мониторинга/управления от подключенного к нему O-RU, что освобождает NMS от функций 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 выполняет функцию клиента NETCONF, а O-RU – сервера 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 NETCONF, а O-RU – сервера NETCONF.

Сокращения и обозначения на рис.4:

- **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



Источник: WP "Security in Open RAN", Altiostar, 2021; https://www.altiostar.com/white-paper-security-in-open-ran/

Рис.4. 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);

- **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, SIB1 и сообщения системной информации (System Information, SI);
- **IPSec** (IP Security): набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет подтверждать подлинность (аутентификацию), 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;
- **PDU** (protocol data unit): обобщенное название фрагмента данных на разных уровнях модели OSI: кадр Ethernet, IP-пакет, UDP-датаграмма, TCP-сегмент и т. д.;
- **5GC**: опорная (Core) сеть 5G;
- **UPF** (User Plane Function): одна из сетевых функций (Network Functions, NF) уровня ядра (Core) сети 5G (5GC). UPF отвечает за маршрутизацию и пересылку пакетов, проверку пакетов, обработку QoS и внешний сеанс PDU для соединения сети передачи данных (DN) в архитектуре 5G;
- **DU** (Destributed Unit): распределенный блок, часть функциональности BBU;
- **CU** (Centrlized Unit): централизованный блок, часть функциональности BBU;
- **SMO** (Service Management and Orchestration system): система управления и оркестрации при предоставлении услуг/сервисов;
- **M-plane** (Management plane): уровень управления сетью – соединение между открытым радиоблоком O-RU и открытым распределенным блоком O-DU;
- **CUS-plane** (Control user synchronization plane): уровень синхронизации – многофункциональный интерфейс используется для передачи сигналов управления и пользовательских данных соответственно, обеспечивает синхронизацию действий между несколькими устройствами радиодоступа;
- **TLS** (Transport Layer Security): протокол защиты транспортного уровня, стандартный

Таблица 2. 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

протокол, который используется для создания защищенных онлайн-соединений;

- **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** (F1 Application Protocol, F1AP, 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;
- **F1-U** (F1 Application Protocol, F1AP, user plan): прикладной интерфейс / протокол F1AP (F1 Application Protocol, F1AP) в соответствии с 3GPP TS 38.473 version 15.3.0 Release 15. В примере на рис.4 передается поверх протокола IPsec.

В табл.2 представлены наиболее значимые угрозы для основных компонентов сети 5G.

Сокращения и обозначения в табл.2:

- **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 способности, 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 мобильной связи 5G должны стать для предприятий и организаций, а также частных пользователей надежной, пользующейся доверием инновационной платформой, нацеленной на создание и предоставление новых услуг. В ближайшем будущем эти сети будут служить основным инструментом для оцифровки и модернизации важнейших национальных инфраструктур в сфере энергетики, транспорта и т.д. Высокая надежность и устойчивость к внешним атакам напрямую связаны с безопасностью оказания услуг на сетях мобильной связи 5G.

Литература

1. Журнал "Открытые Системы. СУБД". Безопасность 5G. [Электронный ресурс]. URL: https://www.osp.ru/os/2020/02/13055462/ (дата обращения: 08.10.2021).
2. Рекомендация Международного союза электросвязи МСЭ-Т Е.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 электросвязи МСЭ X.805 Security architecture for systems providing end-to-end communications (10/2003) (Series X: Data Networks and Open System Communications. Security).
4. Рекомендация Международного союза электросвязи 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]. URL: https://www.ericsson.com/en/security/a-guide-to-5g-network-security (дата обращения: 08.10.2021).
6. WP Security in Open RAN, Altiostar. [Электронный ресурс]. URL: https://www.altiostar.com/white-paper-security-in-open-ran/ 2021 (дата обращения: 08.10.2021).
7. Как обеспечить безопасность сетей 5G. Cnews. [Электронный ресурс]. URL: https://safe.cnews.ru/articles/2020-11-20_kakie_ugrozy_bezopasnosti_nesut (дата обращения: 08.10.2021).