СЕТИ 5G: обеспечение конфиденциальности и безопасности

Часть 1

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

УДК 004.056.53, DOI: 10.22184/2070-8963.2021.99.7.74.79

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, к управлению транспортными средствами и т. п. В статье рассмотрены вопросы обеспечения безопасности и защиты конфиденциальных данных при оказании телекоммуникационных услуг на базе сетей 5G. В первой части материала основное внимание уделено теме международной стандартизации обеспечения безопасности телекоммуникационных сетей.

Телекоммуникационные сети и вопросы безопасности

Телекоммуникационные сети хранят и передают данные о местоположении и конфиденциальную информацию, например сообщения и голосовые разговоры правительственных чиновников, лиц, принимающих решения. Государственные субъекты (или субъекты, поддерживаемые государством) всегда были заинтересованы в том, чтобы следить за действиями других государств.

Социальная, экономическая и политическая деятельность все чаще перемещается в цифровое пространство, в котором данными обмениваются через общедоступные телекоммуникационные сети. Туда же переносятся операции по сбору информации, представляющей большой интерес для разведывательных организаций из разных уголков мира.

Промышленный шпионаж также мигрирует в цифровую сферу, поскольку все больше и больше ценных активов компаний создаются, хранятся и передаются в цифровом виде. Цель состоит в том, чтобы получить доступ к коммерческой тайне компании (включая финансовую документацию и информацию о ценах, конфиденциальную информацию о клиентах), а также к интеллектуальной собственности, в том числе данным о новых технологиях или инновациях. Объединяющим фактором служит намерение субъекта использовать информацию для изменения конкурентной ситуации в свою пользу.

Безопасность актуальна для всех критически важных сетей, включая:

- корпоративные местные и глобальные сети;
- межведомственные правительственные сети;
- взаимодействие ЦОД;
- инфраструктуру умного города, в том числе управление городским транспортом, датчиками, системами видеонаблюдения, системой безопасности населенных пунктов и т. п.;
- финансы и коммерцию, в том числе взаимодействие главных и периферийных офисов банков, а также бизнес-подразделений крупных и средних компаний, биржевые операции и т. п.;
- здравоохранение, в том числе телемедицину и телездравоохранение;
- коммунальные услуги, включая умные сети, датчики, телезащиту и т. п.;
- системы городского и междугородного транспорта, в том числе сигнализацию железных и автомобильных дорог, газо- и нефтетрубопроводов, электрических сетей, систем водо-, электроснабжения и т. п.

Понимание безопасности на этапе эволюции к сетям мобильной связи 5G

Телекоммуникационные сети быстро развиваются в технологической среде, которая может включать виртуализацию, Интернет вещей и другие технологические достижения, подразумеваемые под "Индустрией 4.0".

Ожидается, что прогресс в области технологий, а также широкое развитие сетей радиодоступа 5G и более высоких поколений окажут значительное влияние на безопасность при внедрении таких решений, как, например, программно-определяемые сети (SDN), виртуализация сетевых функций (NFV) и обеспечение периферийных вычислений (Edge computing). Достаточно гибкий стандарт 5G 3GPP учитывает различные типы физического и виртуального перекрытия между сетью радиодоступа (RAN) и ядром сети (Core) на всем протяжении от удаленного клиентского устройства до ядра сети.

Сети нового поколения должны блокировать слежку с использованием International Mobile Subscriber Identity (IMSI) – международного идентификатора мобильного абонента. Этот способ проникновения предполагает наличие специального устройства, которое имитирует сигнал вышек сотовой связи, чтобы обмануть телефоны в районе покрытия.

В связи с введением шифрования IMSI эволюция к 5G знаменует начало новой эры сетевой безопасности. Все данные трафика, которые передаются по радиосети 5G, зашифрованы, защищены целостностью и подлежат взаимной аутентификации, включая устройства, подключаемые к сети. Используются надежные методы шифрования; сервисная архитектура, где компоненты аутентифицируют друг друга одновременно; эластичная безопасность, которая может смешивать сотовую и несотовую среду посредством аутентификации; шифрование идентификаторов конечной точки, а также улучшение сигнализации посредством TLS-протокола защиты транспортного уровня.

TLS (Transport Layer Security) представляет собой стандартный протокол, который применяется в целях создания защищенных онлайн-соединений и дает возможность клиентам проверять подлинность серверов. С его помощью серверы выполняют проверку подлинности клиентов (когда это важно). Протокол TLS позволяет также создать защищенный канал посредством кодирования всех передаваемых данных.

Однако механизм обеспечения безопасности 5G посредством шифрования IMSI станет доступен только с внедрением ядра сети 5G (5GC), что запланировано многими операторами. Обусловлено это тем, что большая часть передовых механизмов безопасности реализуется на уровне ядра сети 5G. В автономной архитектуре (только система 5G) используются как сеть радиодоступа (RAN), так и ядро (Core) сети 5G, что позволяет в полной мере реализовать архитектурные компоненты безопасности.

В настоящее время в большей части эксплуатируемых по всему миру сетей 5G реализована неавтономная архитектура, то есть совмещение систем 4G и 5G. При использовании такой архитектуры применяются существующие механизмы безопасности LTE (4G), что ограничивает возможности реализации всех преимуществ нового поколения сети мобильной связи, особенно в части минимизации задержек и повышения надежности передачи данных.

К сети 5G может быть подключен широкий круг устройств разного рода. Разработчики стандартов 5G предусмотрели возможность подключения к сетевой инфраструктуре не менее 1 млн устройств в расчете на квадратный километр.

Таблица 1. Особенности безопасности сетей 5G

Особенность	Пояснение	Влияние на безопасность
Скорость и задержка	Более высокие скорости передачи клиентского трафика: если в сетях 4G скорость до 100 Мбит/с, то в сетях 5G – до 5–10 Гбит/с. Меньшее значение задержки: в 4G порядка 50 мс, в 5G – не более 1–2 мс	Злоумышленники могут получать данные от взломанных устройств быстрее и устраивать более масштабные DDoS-атаки. Взломщики обретают более широкие технические возможности
Передача и хранение данных	Собираемые данные чаще хранятся на периферии, а не централизованно	На периферии уровень безопасности может быть ниже, чем в центре. Атакующие способны устанавливать бэкдоры[1] на мобильные базовые станции, чтобы перехватывать данные непосредственно в точках доступа к радиосети
Использование SDN, искусственного интеллекта, машинного обучения	SDN и искусственный интеллект используются для реализации функций разных систем и обеспечивают нужные показатели скорости и задержки	В системах искусственного интеллекта могут быть бреши. В случае компрометации SDN-контроллера взломщик получает доступ к управляемому им устройству
Сегментирование сети (slicing)	Сеть может быть разделена на логические сегменты, предоставляющие разные сервисы	В зависимости от потребностей пользователей можно гибко менять доступные им уровни безопасности
Подключаемые устройства	Если в 4G работают преимущественно мобильные телефоны, то в 5G – более широкий круг устройств	Поверхность атаки может увеличиться. У недорогих устройств, соединенных с сетью, часто отсутствуют необходимые средства защиты
Специфика применения	Возможны варианты узкоспециализированного применения	Взлом критически важных систем может иметь катастрофические последствия. Злоумышленникам доступны более широкие технические возможности

[1] Бэкдор – тайный вход (от англ. back door – черный ход, или буквально "задняя дверь") – дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом.

По мере увеличения числа недорогих слабозащищенных устройств в сетях 5G расширяется и поверхность атаки, поскольку большую часть таких устройств нельзя оснастить межсетевым экраном (firewall) ввиду недостаточной емкости памяти. Однако, благодаря возможностям SDN, сеть 5G можно разделить на несколько сегментов, оптимизированных для выполнения различных задач (slicing). При этом для каждого сегмента можно предусмотреть свои возможности обеспечения безопасности. Например, системы связи для экстренных служб могут быть защищены лучше, чем платформы онлайн-игр. Особенности безопасности сетей 5G представлены в табл.1 [1].

Стандартизация как важнейший процесс определения безопасности телекоммуникационной сети

Стандартизация – это процесс, посредством которого операторы, поставщики услуг и оборудования, а также другие заинтересованные стороны устанавливают стандарты совместной работы сетей по всему миру. Сюда входят также вопросы защиты сетевой инфраструктуры и пользователей от злоумышленников. Необходимы договоренности о том, как сети по всему миру будут работать вместе и как обеспечить безопасность сетевой инфраструктуры и пользователей.

В рекомендацию 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) включены следующие положения по обеспечению безопасности телекоммуникационных сетей:

- только законные субъекты должны иметь доступ к телекоммуникационным сетям;
- законные субъекты должны иметь возможность работы с сетевыми ресурсами, к которым им разрешен доступ;
- сети электросвязи должны обеспечивать конфиденциальность на уровне, установленном политиками безопасности сети;
- все участники должны нести ответственность за свои действия в телекоммуникационных сетях;
- для обеспечения высокой надежности телекоммуникационные сети должны быть защищены от нежелательного доступа или операций;
- должна быть предусмотрена возможность получения из сетей электросвязи информации, связанной с безопасностью (но поступление такой информации должно быть доступно только законным субъектам);
- в случае обнаружения нарушений безопасности с ними следует обращаться контролируемым образом в соответствии с заранее определенным планом, чтобы минимизировать потенциальный ущерб;
- должна быть обеспечена возможность восстановления нормальных уровней безопасности после обнаружения нарушений или вторжений, включая несанкционированный доступ к сетевым ресурсам;
- архитектура безопасности сетей электросвязи должна обеспечивать определенную гибкость для поддержки различных политик безопасности.

В соответствии с рекомендацией МСЭ-Т Е.408 [2] для эффективной защиты сети рекомендуется использовать несколько уровней безопасности, причем чем больше организовано таких уровней, тем эффективнее защищенность инфраструктуры. В рекомендации упомянуты и прокомментированы следующие шесть уровней безопасности.

1. **Уровень системных / сетевых администраторов** – самый важный актив в области сетевой безопасности. Системный администратор отвечает за стабильное и безотказное функционирование ИТ-инфраструктуры, настройку сетей, мониторинг, следит за безопасностью данных, а также проводит инвентаризацию и обновление программного обеспечения. Сетевой администратор (администратор вычислительной сети) отвечает за работу компьютерной сети предприятия в штатном режиме.

   Отмечается, что ежегодные дополнительные траты на хорошего системного администратора более эффективны, чем покупка дорогой системы сетевого экранирования типа firewall. Хорошие системные / сетевые администраторы глубоко понимают операционные системы, с которыми работают; знают, как заблокировать каждый сетевой элемент, чтобы разрешить только процессы и порты узла, относящиеся к обработке этих данных.
2. **Уровень физической безопасности.** Каждый злоумышленник в мире знает, что самый простой способ получить доступ к сети – проникнуть изнутри. Слишком много случаев социальной инженерии, когда злоумышленники просто звонили в службу поддержки и упоминали, что забыли свой пароль, просили службу поддержки изменить его на новое значение xxxxx. Физическая безопасность включает в себя все процессы: от предоставления доступа к блокам и полкам (консолям) только определенным людям (например, системным администраторам) до приведения в действие политик в отношении того, какая информация об организации сети предоставляется общественности. Правильные политики допустимого использования ресурсов сети, а также политики назначения паролей и установки ПО во многом помогают организациям заблокировать несанкционированный доступ к своим сетям.
3. **Уровень мониторинга.** Очень редко атака оказывается успешной с первой попытки. Большинство атак можно остановить, если проверять журналы системы хотя бы раз в день. Это займет не так много времени, как кажется на первый взгляд. Человеческий глаз – лучшее средство для выявления закономерностей в файлах журналов. Существует несколько хороших программ, которые отслеживают файлы журналов. Хотя эти программы могут быть очень полезными, системный администратор должен каждый день читать журналы

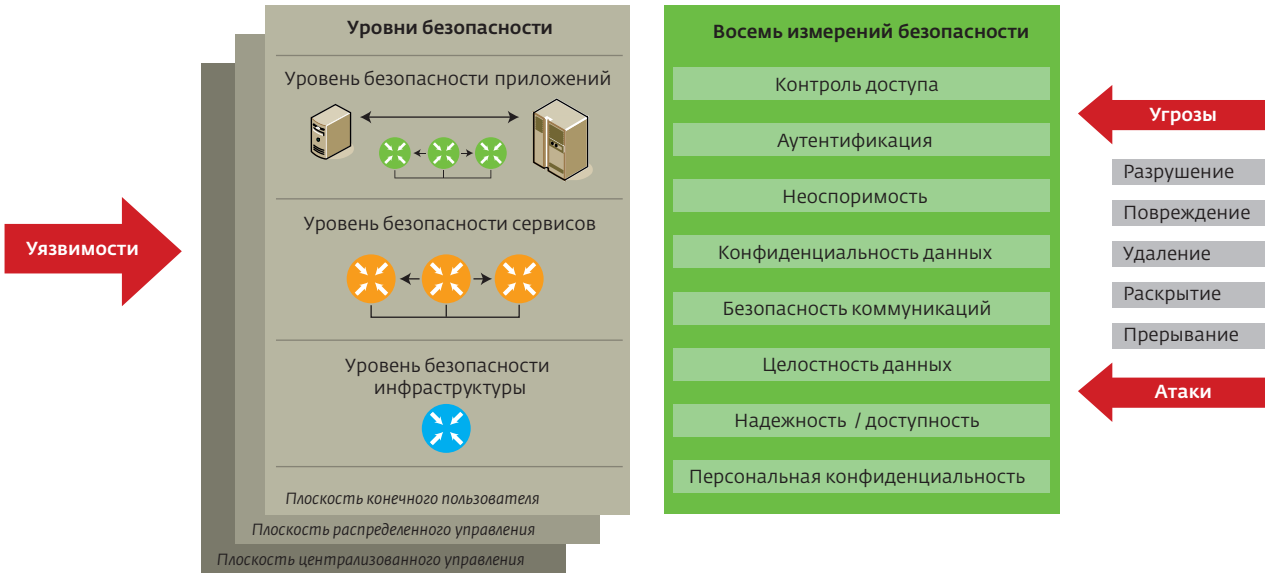

Рис.1. Архитектура обеспечения сквозной безопасности сети (end-to-end) по рекомендации МСЭ X.805

фиксации событий на устройствах, относящиеся к его компетенции.

4. **Уровень телекоммуникационного программного обеспечения.** Каждое ПО, устанавливаемое на серверы, следует оценивать с учетом требований безопасности. Системный администратор должен знать, например, какие порты TCP и UDP будет прослушивать программное обеспечение, с какими учетными записями пользователей оно взаимодействует и какие права доступа к каталогам требуются для этого ПО. Кроме того, перед приобретением рекомендуется поискать в программном обеспечении ошибки, влияющие на безопасность. Такой порядок действий должен стать частью процесса оценки всего приобретаемого ПО.
5. **Уровень программных инструментов (tools) безопасности.** После того, как для вышеупомянутых четырех уровней установлены надлежащие политики и практики, необходимо изучить межсетевые экраны (firewalls) ПО, включая прокси-серверы, для обнаружения несанкционированного доступа или попыток его реализации. После взлома firewalls все серверы открываются для атак.
6. **Уровень аудита безопасности.** Обеспечение сетевой безопасности подразумевает наличие непрерывно изменяющейся цели. Каждый день кто-то где-то находит новый метод взлома безопасности сети. Поэтому важно, чтобы организации регулярно проверяли свою сеть. Аудит должен проводиться по всем аспектам сетевой безопасности на почтовом сервере, DNS, домене, веб-серверах и FTP-серверах. В частности, целесообразно регулярно проверять устойчивость сети к физическим атакам.

В рекомендации 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) определена архитектура безопасности для обеспечения сквозной сетевой безопасности. В соответствии с этой рекомендацией сложный набор функций, связанных с безопасностью сети, подразделяется на следующие архитектурные компоненты:

- расчет безопасности (Security Dimensions) – набор мер для решения всех аспектов сетевой безопасности на трех упомянутых ниже уровнях безопасности: приложений (Application security), сервисов / служб (Service security) и инфраструктуры сети (Infrastructure);
- уровни безопасности (Security Layers). В рекомендации [3] указаны три уровня

безопасности, которые опираются друг на друга при предоставлении сетевых решений:

- безопасность приложений (Applications Security Layer);
- безопасность сервисов / служб (Services Security Layer);
- безопасность инфраструктуры (Infrastructure Security Layer);

- плоскости безопасности (Security Plane) – определенный тип сетевой активности, опирающийся на расчеты по безопасности (Security Dimensions). В рекомендации [3] указаны три плоскости:
  - централизованного управления сетью (Management Plane);
  - распределенного управления сетью (Control Plane);
  - конечного пользователя (End-User Plane).

Чтобы обеспечить комплексное решение, меры безопасности (например, контроль доступа, аутентификация) должны применяться к каждому типу сетевой активности.

На рис.1 представлена архитектура обеспечения безопасности сети из конца в конец (end-to-end) по рекомендации МСЭ X.805.

В рекомендацию МСЭ-Т E.408 [2] включен обзор требований безопасности и структуры, определяющие угрозы безопасности для телекоммуникационных сетей в целом (фиксированных и мобильных, для передачи голосовых сообщений и данных). В этом же документе приведены требования к планированию контрмер, которые могут быть приняты для снижения рисков. Данные требования носят общий характер.

Серия рекомендаций Международного союза электросвязи МСЭ M.3016.x (X=0/1/2/3/4) определяет требования безопасности для систем управления телекоммуникационной сетью. В частности, в рекомендацию МСЭ M.3016.1 Security for the management plane: Security requirements (04/2005) (Series M: Telecommunication Management, Including TMN and Network Maintenance Telecommunications management) включен набор требований, услуг и механизмов для обеспечения безопасности функций управления, необходимых для поддержки инфраструктуры электросвязи. Особое внимание уделяется общим вопросам безопасности на физическом и логическом уровнях сети. ■

Сеть связи самого длинного в мире аммиакопровода модернизирована на основе российского оборудования DWDM

Компания "Т8" завершила работы по запуску каналов связи магистральной технологической сети для ПАО "Трансаммиак". Переход с медной инфраструктуры на волоконно-оптическую сеть с применением технологии спектрального уплотнения (DWDM) стал одним из этапов масштабной модернизации самого длинного в мире аммиакопровода.

На DWDM-оборудовании "Волга" построена 40-канальная сеть длиной 1500 км и пропускной способностью 10 Гбит/с, работающая по одной паре волокон. Всего было объединено 14 узловых точек, включая насосные и другие объекты от Тольятти до Россоши Воронежской области.

Оптическая сеть объединяет все системы магистрального аммиакопровода и обеспечивает передачу данных:

- телемеханика и контроль состояния трубопровода;
- работа системы оповещения населения о чрезвычайных ситуациях;
- связь между объектами;
- удаленное видеонаблюдение с промежуточных станций и объектов.

Аммиакопровод – это сложный технологический комплекс, который требует стабильной и надежной работы всех компонентов на долгие годы, поэтому при проектировании сети была заложена возможность расширения пропускной способности каналов до 100 Гбит/с на существующей оптической инфраструктуре. Еще одной отличительной особенностью проекта стала система управления с георезервированием, которая обеспечивает высокую степень надежности всей сети.

По информации ООО "Т8"

Запущена первая в России межвузовская квантовая сеть

В Москве запущена экосистемная межвузовская квантовая сеть с открытым доступом, которая объединила кампусы НИТУ "МИСиС" и МТУСИ. Это первая российская площадка для реализации решений в сфере защиты данных с применением квантовой криптографии. Проект по созданию сети реализуется участниками консорциума Центра компетенций НТИ "Квантовые коммуникации", созданного на базе НИТУ "МИСиС": МТУСИ, ООО "КуРэйт", ООО "Код Безопасности".

Межвузовская квантовая сеть состоит из пяти узлов, расположенных в корпусах НИТУ "МИСиС" и МТУСИ, она имеет открытую архитектуру и масштабируется. Доступ к сети получают вузы, научные организации, индустриальные партнеры, госучреждения и стартапы. На базе сети они могут разрабатывать современные софтверные приложения в сфере информационной безопасности с применением квантовых ключей.

В планах консорциума Центра НТИ – привлечь новых участников, которые могут подключиться к сети. Вместе они смогут доработать архитектуру квантовой сети до "кольца", что даст новые возможности для ее развития.

По информации МТУСИ

ТЕХНОСФЕРА
РЕКЛАМНО-ИЗДАТЕЛЬСКИЙ ЦЕНТР

100% ГАРАНТИЯ
ПОЛУЧЕНИЯ ВСЕХ НОМЕРОВ

Стоимость 2200 р. за номер
Периодичность: 10 номеров в год
www.electronics.ru

Стоимость 1430 р. за номер
Периодичность: 8 номеров в год
www.photonics.su

Стоимость 1430 р. за номер
Периодичность: 6 номеров в год
www.j-analytics.ru

ПОДПИСКА НА ЖУРНАЛЫ

www.technosphera.ru

Стоимость 1056 р. за номер
Периодичность: 8 номеров в год
www.lastmile.su

Стоимость 1287 р. за номер
Периодичность: 8 номеров в год
www.nanoindustry.su

Стоимость 1716 р. за номер
Периодичность: 4 номера в год
www.stankoinstrument.su