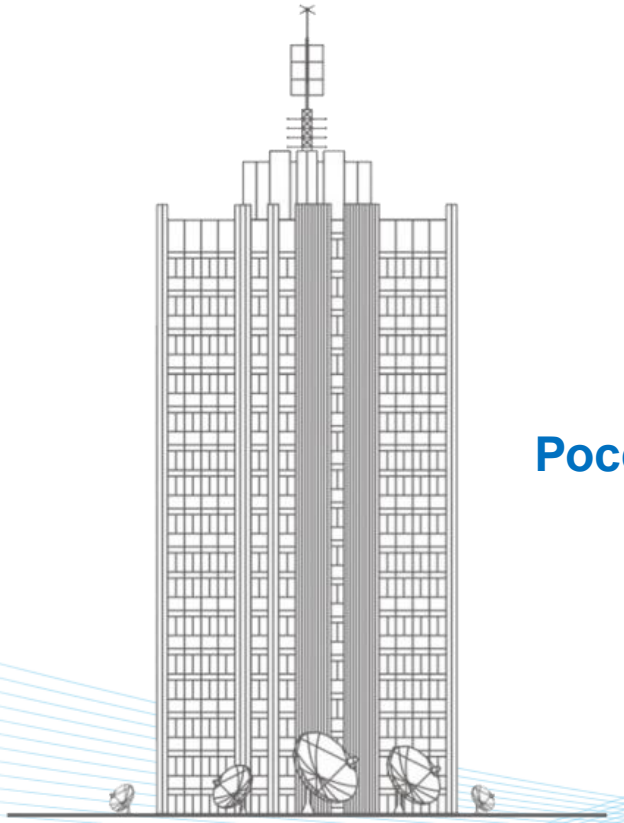


Создание и развитие сетей 5G/IMT-2020 в Российской Федерации, проблемы и их решение

Гасс Яков Маркович
Начальник лаборатории НТЦ Анализа ЭМС

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
РОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ РАДИО
имени М.И. КРИВОШЕЕВА

Актуальность обеспечения информационной безопасности на сетях 5G

- применение сетей 5G в сфере ЖКХ (управление газовым хозяйством, управление подачей электроэнергии, управление системами контроля и т. д.)

- применение сетей 5G на различных предприятиях, технологические процессы которых потенциально несут существенные угрозы техногенных и экологических катастроф (ТЭК, металлургия, строительство, различные производства и т. д.)

- Передача данных (медицина, финансы и коммерческая деятельность, транспорт и т. д.)

Обеспечение информационной безопасности сетей 5G

Направления обеспечения ИБ сетей 5G

Отказоустойчивость

- Cloud RAN – архитектура
- Формирование сетевых «срезов»
- Поддержка одинаковых конфигураций БС в режиме «хендовера»

Безопасность соединений в сети

- Шифрация трафика и обеспечение целостности сообщений
- Разделение ключа безопасности между различными функциями опорной сети
- Автоматическое восстановление алгоритмов безопасности после сбоев

Управление идентификаторами абонента

- Улучшенные методы аутентификации
- Возможность определения местонахождения абонента во время прохождения аутентификации

Обеспечение безопасности оборудования

- 3GPP и GSMA разработана схема (NESAS), определяющая требования по безопасности сетевого оборудования и правила проведения аудита инфраструктуры производителя оборудования

Защита передаваемых абонентом данных

- Способность выявления «ложных» БС
- Периодическое обновление временных идентификаторов абонента
- Повышенная защищенность данных абонента в режиме роуминга

Объекты информационной безопасности в сетях связи 5G

Аппаратные средства

- Выносной радиоузел (DU, RU)
- ЦОД различного уровня в составе:
  - Серверное оборудование
  - Коммутаторы плоскости инфраструктуры
- Абонентские устройства
- USIM-карты
- Оборудование изготовления и программирования USIM-карт

Программные средства

- Сетевые функции, запускаемые на виртуальных машинах на серверах
- Общее ПО оркестраторов
- ПО SDN контроллеров
- Общее ПО серверов
- Общее ПО коммутаторов
- Общее и специальное ПО радиоузлов
- Общее и специальное ПО оборудования пользователя (UE)
- Общее и специальное оборудование ПО USIM-карт
- Общее и специальное ПО оборудования изготовления и программирования USIM-карт

Возможные способы противодействия атакам

- использование в составе программно-аппаратных комплексов сетей связи вычислительных средств, на которые имеется заключение об отсутствии недекларированных возможностей в их аппаратной платформе, а также BIOS и встроенном ПО;

- использование в программно-аппаратных комплексах сетей связи системного и прикладного ПО, на которое имеется заключение об отсутствии недекларированных возможностей;

- применение в ходе эксплуатации программно-аппаратных комплексов сетей связи процедур контроля целостности аппаратных средств, а также системного и прикладного ПО;

- применение СКЗИ, обладающих необходимым быстродействием и обеспечивающих «быстрое» выполнение алгоритмов ГОСТ Р 34.10-2012 «Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.11-2012 (Функции хеширования), ГОСТ Р 34.12-2015 (блочные шифры – Магма и Кузнечик).

Варианты государственной поддержки

Поощрение инвестиций в сети 5G

- формирование благоприятной среды для инвестиций
- создание специальной системы поддержки инновационных проектов
- введение налоговых льгот

Упрощение регуляторики

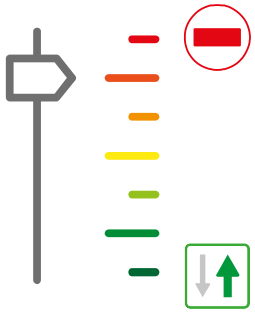
- введение технейтральности для повышения эффективности использования РЧС
- введение сетевой нейтральности для возможности работы с большими данными и выполнения требований по защите конфиденциальной информации
- разработка нормативной базы для сертификации новых типов оборудования
- упрощение доступа к федеральным и муниципальным инфраструктурным объектам
- упрощение процессов стандартизации и получения разрешений

Снижение размеров ежегодной и разовой платы за пользование спектром

Обеспечение защиты населения от электромагнитного излучения (ЭМИ)

Факторы повышения экономико-социальной значимости вопросов защиты населения от ЭМИ в России

- Действие устаревших норм СанПин и МУК, определяющих защиту населения от ЭМ излучения.



- Отсутствие значений предельно-допустимых уровней (ПДУ) на частотах выше 2400 МГц.

Факторы, которые должны быть учтены при переработке норм СанПИН и МУК

- Учет воздействия излучений сетей мобильной связи, основанных на перспективных стандартах.

- Воздействие электромагнитного излучения, создаваемого РЭС в закрытых помещениях (in-door).

- Учет совокупного воздействия электромагнитных излучений, создаваемых несколькими РЭС различных стандартов.

Диапазоны радиочастот для сетей 5G в Российской Федерации

Сейчас

- полоса радиочастот шириной 400 МГц 24,25 – 24,65 ГГц, в том числе для технологических 5G NR сетей (Решение ГКРЧ от 17.03.2020 г. № 20-54-02);
- полоса радиочастот 4,8-4,99 ГГц для пилотных зон (Решение ГКРЧ от 24.12.2018 г. № 18-48-02);
- полоса радиочастот 25,25-27,5 ГГц для пилотных зон (Решение ГКРЧ от 25.07.2019 г. № 19-51-01).

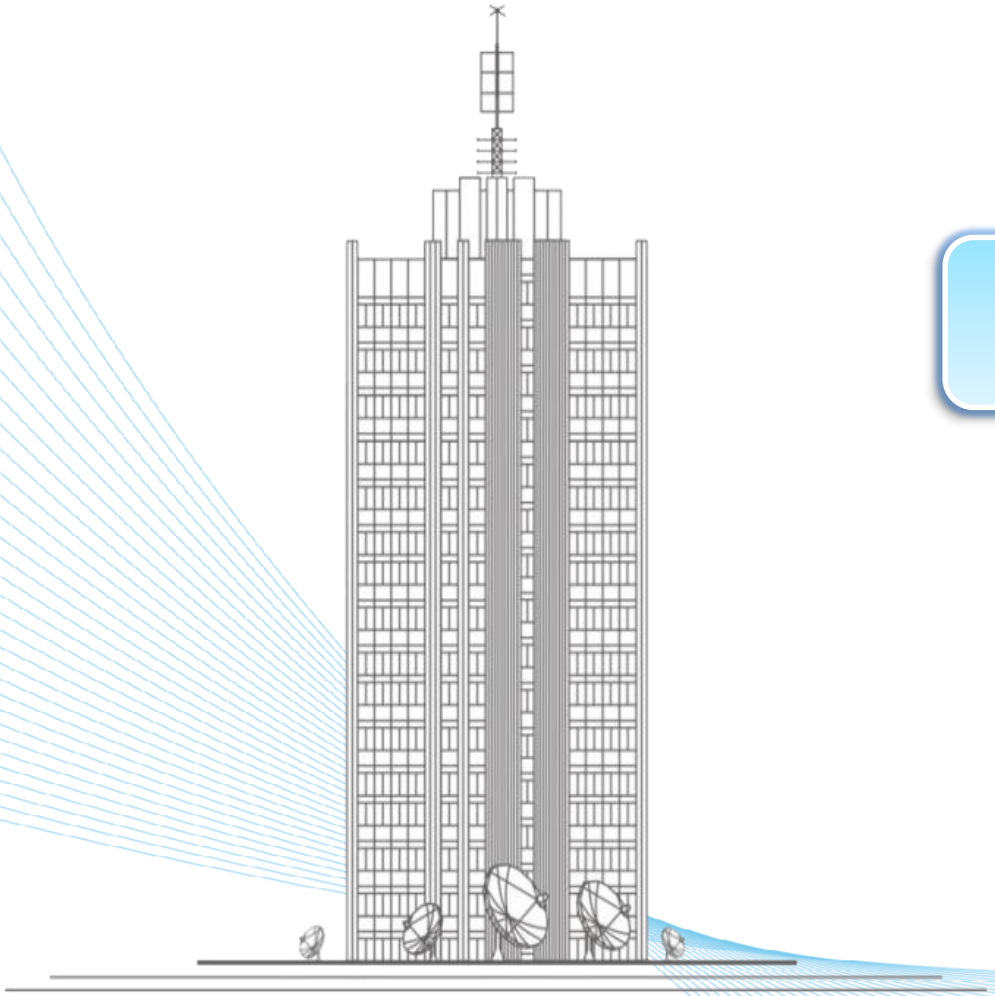
В ближайшие годы

- высвобождение 2*20 МГц в диапазоне 700 МГц за счет конверсии к 2023 г.;
- введение режима технологической нейтральности для сетей 5G в диапазонах 1800 – 2600 МГц в 2021 г.;
- выделение новых полос радиочастот в диапазоне 24,25 – 27,5 ГГц.

В перспективе

- выделение полос радиочастот в диапазоне 6425 – 7100 МГц в случае его распределения сетям 5G на ВКР-23.

В ближайшие годы планируется выделение РЧС сетям 5G во всех диапазонах радиочастот, необходимых для эффективного предоставления услуг и приложений сетей 5G всех типов



БЛАГОДАРЮ ЗА ВНИМАНИЕ!