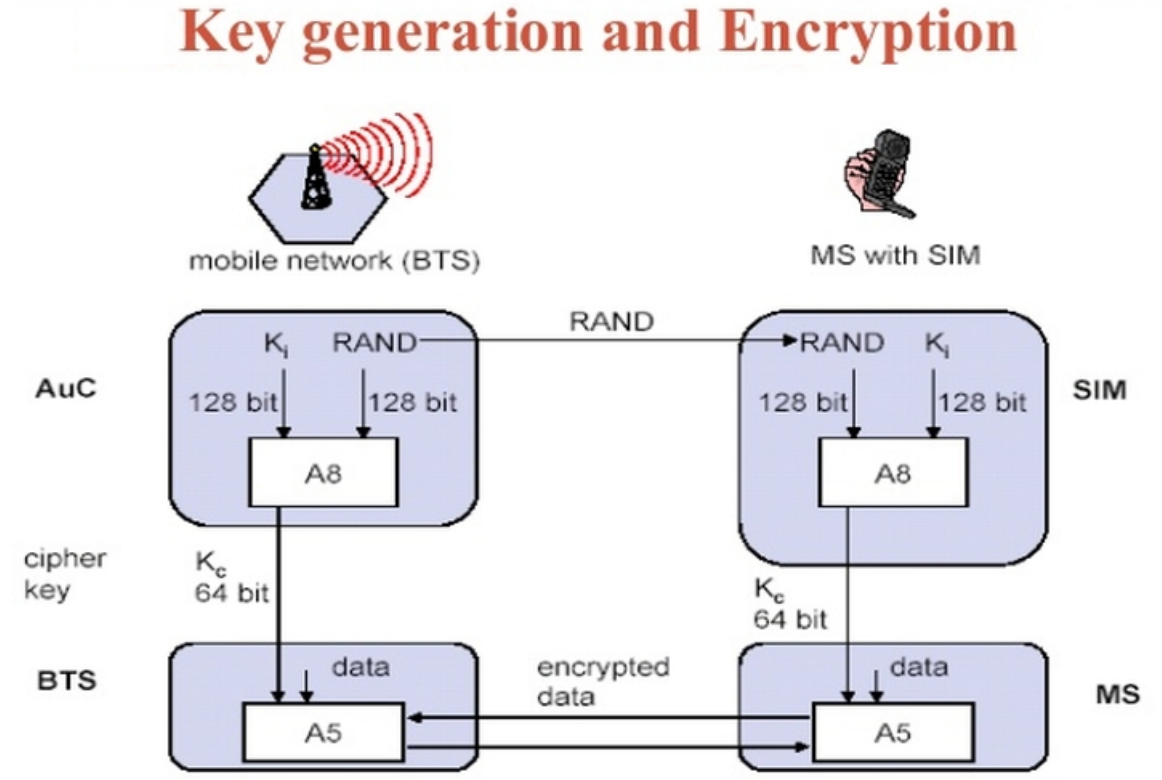
Минкомсвязь: переход на российские криптоалгоритмы усилит защиту сотовых сетей от несанкционированного доступа

Ссылаясь на ПП РФ от 25 июня 2009 года №532, в котором перечислены средства связи, подлежащие обязательной сертификации, Минкомсвязь изменило требования к отдельным модулям оборудования коммутации сетей сотовой связи, потребовав применения российских алгоритмов шифрования в процедурах аутентификации и идентификации абонентов. Цель – "защитить сети связи от вредоносных действий зарубежных спецслужб".

В конце прошлого года Министерство связи и массовых коммуникаций разработало и представило* на портале regulation.gov.ru проект приказа об изменениях в правилах применения оборудования коммутации в сетях LTE ("Правила..." утверждены приказом Минкомсвязи №130 от 6 июня 2011 года) и в правилах применения оборудования коммутации в сетях стандартов UMTS и/или GSM 900/1800 ("Правила ..." утверждены приказом Минкомсвязи №160 от 27 июня 2011 года).

С какой целью обновят приказы Минкомсвязи

Предложенные изменения должны увеличить защищённость российских сетей сотовой связи от несанкционированного доступа к ним и передаваемой по ним информации за счёт внедрения сертифицированных по требованиям безопасности средств криптографической защиты информации с использованием отечественных алгоритмов шифрования. Эта замена необходима для защиты от возможных вредоносных действий зарубежных спецслужб, которые могут использовать центры аутентификации пользователей услугами связи (HLR/AuC) иностранного производства для доступа к сетям связи и передаваемым по ним сообщениям пользователей услугами связи, носящим конфиденциальный характер. Полученная информация может быть использована для нанесения значительного вреда безопасности государства. В применении российской криптозащиты заинтересовано не только государство, но и сотовые операторы связи, так как они могут снизить свои издержки, связанные с нарушением функционирования сетей связи. Такое обоснование представили разработчики проекта приказа Минкомсвязи.



Для беспокойства есть причины. Например, в 2015 году в СМИ появилась информация об успешной атаке компьютерной сети крупнейшего производителя SIM-карт компании Gemalto. Её продукцию покупают сотни операторов связи из разных стран мира. Gemalto после внутренней проверки заявила, что факт кражи информации не подтвердился.


ТАСС ИНФОРМАЦИОННОЕ АГЕНТСТВО РОССИИ

Документы Сноудена: спецслужбы США и Великобритании выкрали шифры у производителя SIM-карт

Международная панорама 20 февраля 2015, 0:31 UTC+3

По данным СМИ, разведывательные ведомства получили возможность тайно отслеживать телефонные разговоры, не запрашивая на это разрешения

НЬЮ-ЙОРК, 19 февраля. /Корр. ТАСС Андрей Бекренев/. Агентство национальной безопасности (АНБ) США, занимающееся электронной разведкой, и Управление правительственной связи (УПС) взломали компьютерные сети крупнейшего в мире производителя SIM-карт и похитили ключи шифрования, используемые для защиты разговоров по сотовым телефонам от несанкционированного доступа. Об этом говорится в секретных документах спецслужб Великобритании, переданных СМИ бывшим сотрудником ЦРУ и АНБ Эдвардом Сноуденом и опубликованных интернет-изданием The Intercept.

Ранее были выявлены слабые места в системе безопасности, позволяющие в "домашних условиях" создавать клоны SIM-карт.

Что предложено изменить

В соответствии с первоначальной** версией проекта приказа с 1 декабря 2019 года можно будет в сетях LTE эксплуатировать сервер абонентских данных и/или центр аутентификации (Home Subscriber Server / Authentication Center, далее – HSS/AuC) только в случае наличия сертификата соответствия средств криптографической защиты требованиям ФСБ к шифровальным (криптографическим) средствам класса КА. Аналогичные требования к СКЗИ будут действовать и для сетей подвижной радиотелефонной связи стандартов GSM/UMTS.

В ведомственном документе изложены "Требования к протоколу взаимодействия опорного регистра местоположения HLR и/или центра аутентификации AuC с отдельным аппаратным модулем безопасности HSM, выполняющим криптографические функции аутентификации абонентов". Так как оборудование коммутации сетей подвижной радиотелефонной связи включено в перечень средств связи, подлежащих обязательной сертификации, то операторы российских сетей сотовой связи до 1 декабря 2019 года должны будут произвести изменения, чтобы в процедурах аутентификации и идентификации абонентов применялись средства криптографической защиты информации класса КА для оборудования коммутации узлов связи. Эти средства криптозащиты должны соответствовать требованиям, установленным ФСБ.



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер _____ от "____" _____ 201__ г.

Действителен до "____" _____ 202__ г.

Выдан _____

Настоящий сертификат удостоверяет, что _____

_____

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, _____

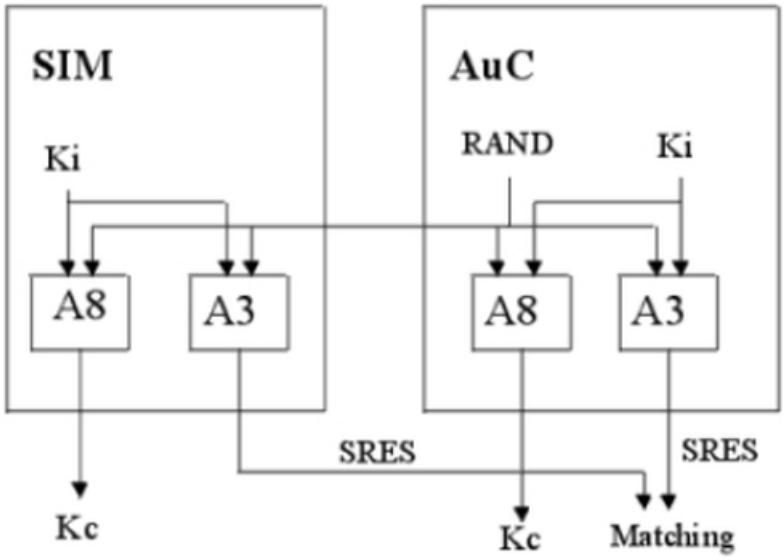
Разработчики нормативного акта заявили, что единовременные расходы изготовителей средств связи, связанные с необходимостью их сертификации, составляют ориентировочно 0,5% от стоимости партии готовой продукции. Периодические расходы не предполагаются.

Планируется производство отдельных модулей HSM (Hardware Security Module – аппаратный модуль безопасности), реализующих российские алгоритмы шифрования, кроме проведения обязательной сертификации средств криптографической защиты информации (СКЗИ) центра аутентификации AuC иностранных производителей на соответствие требованиям ФСБ. Разработка и тестирование средств криптографической защиты на специально созданных сегментах сети связи будут выполнены в следующем году. До 1 декабря 2019 года должно хватить времени и на доработку модулей HSM.

В процессе публичного обсуждения были высказаны опасения по поводу беспроблемного перехода на СКЗИ с отечественными алгоритмами шифрования. Представители Минкомсвязи ответили, что эксплуатация существующих устройств AuC будет продлена до момента готовности к переходу на российские модули HSM.

Единовременная замена всех 260 миллионов SIM-карт не планируется

С 1 декабря 2019 года может вступить в силу ещё и обновлённый приказ Министерства информационных технологий и связи Российской Федерации от 9 января 2008 года № 1 "Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации". В тексте проекта приказа добавлено про объекты связи, относящиеся к критической инфраструктуре, а также предложена замена текущих алгоритмов, используемых в процедурах аутентификации абонентов, на российские с сертификатом ФСБ. Операторы связи для защиты от несанкционированного доступа к информации должны осуществлять процедуры аутентификации и идентификации абонентов с использованием СКЗИ класса КА для оборудования коммутации узлов связи и класса КС3 для модуля идентификации абонентов USIM (R-UIM) в составе абонентского оборудования.



AuC — Authentication Center

A3 - алгоритм вычисления SRES (Signed RESponse), A8 - алгоритм вычисления Kc (Key for ciphering)

Перед подготовкой официального заключения с оценкой проекта нормативного акта Минэкономразвития получило отзывы от ПАО "МТС", ПАО "Вымпелком", ПАО "Мегафон", ПАО "Ростелеком", Международной Академии Связи, а также прошли рабочие совещания с участием представителей Минкомсвязи. В доработанном проекте приказа учли некоторые замечания: например, требования не распространяются на SIM-карты, которые были закуплены оператором связи до вступления в силу изменений в приказе №1 от 9 января 2008 года.

Минэкономразвития в своём отзыве обратил внимание на несколько важных моментов, связанных с затратами операторов в связи с принятием нормативного документа. Во-первых, существующие центры аутентификации (AuC) могли бы эксплуатироваться без замены, а теперь появится необходимость закупки дополнительных модулей AuC и HSM, чтобы обеспечить работоспособность "старых" и "новых" SIM-карт. Согласно оценке ПАО "Мегафон" предположительно HSM придётся приобретать на каждые 10 000 абонентов ввиду технических особенностей хранения данных, а также быстродействия в HSM. Кроме того, в проекте приказа предусматривается класс защиты – КА, реализация которого будет сопряжена с дополнительными организационными и техническими мерами, а также крупными затратами порядка 700 млн. рублей, а совокупные затраты операторов на внедрение проектируемых требований превысят 5 млрд. рублей, согласно оценке ПАО "Вымпелком". Также должно быть обеспечено резервирование модулей HSM для бесперебойной работы.

Изменения требований в части SIM-карт фактически закрепляет использование в устройствах пользователей SIM-карт, в то время как мировым трендом последних лет является отказ от данного формата средств абонентского оборудования. Это грозит тем, что производители устройств с встроенными полнофункциональными модулями сотовой связи и с использованием технологий со встроенными модулями сотовой связи (технологии eSIM и iSIM) не смогут поставлять и реализовывать уже произведенную и поставленную продукцию на российский рынок. Поэтому Минэкономразвития рекомендует Минкомсвязи проработать и нормативно закрепить специальный механизм подтверждения соответствия устройств со встроенными модулями сотовой связи требованиям сертификации.

Учитывая сложности временного, финансового и организационного характера и то, что в настоящее время используется около 260 миллионов SIM-карт, а выдача новых USIM с российской криптографией не будет проходить массово и обязательно, есть смысл определить круг лиц, которым по тем или иным причинам необходимы SIM-карты с определённой степенью криптозащиты, предлагает Минэкономразвития. Такой подход позволил бы операторам связи уменьшить затраты на новое оборудование.

Новая проблема возникает и из-за того, что USIM становится сертифицированным средством криптографической информации, а оборот и применение таких СКЗИ должны соответствовать постановлению Правительства Российской Федерации от 16 апреля 2012 г. № 313 и приказу ФАПСИ от 13 июня 2001 г. № 152, то есть, как минимум, необходимы изменения данных НПА. С учётом изменения статуса USIM, эти карты придётся выдавать, соблюдая процедуры, описанные в инструкции ФАПСИ, что, по мнению операторов, сложно реализовать при работе на

массовом рынке.

Несмотря на упоминание нескольких недоработок и на наличие критических замечаний о существенных дополнительных затратах, в итоге заключение Минэкономразвития положительное, что даёт возможность отправки проекта приказа на регистрацию в Министерство юстиции.

Подготовка внедрения российской криптозащиты в сетях 5G

Если в российских сетях сотовой связи второго и третьего поколения замена иностранных алгоритмов шифрования на отечественные должна произойти по прошествии многих лет эксплуатации, то к появлению сетей 5G органы исполнительной власти в сфере безопасности начали готовиться заранее.

В газете "Ведомости" 20 августа появилась информация о размещении на сайте госзакупок заявки на выполнение в течение сентября-декабря 2018 года научно-исследовательской работы по вопросам информационной безопасности в сетях пятого поколения. Рассмотрение заявок и подведение итогов запланировано на 12 сентября. Начальная (максимальная) цена контракта – три миллиона рублей, источник финансирования – государственный бюджет.

Действительно, на сайте zakupki.gov.ru можно найти заявку №0373100053318000008 от 13 августа 2018 года. Разместило её федеральное государственное казённое учреждение "Войсковая часть 43753", поэтому и оплата из госбюджета. Проект тактико-технического задания есть в составе конкурсной документации, но она отсутствует на сайте госзакупок и по письменному запросу предоставляется в печатном виде по адресу, указанному в извещении о закупке. Особенность – потенциальный участник конкурса на выполнение НИР должен иметь допуск к сведениям, составляющим гостайну (наличие действующей лицензии на право осуществления работ со сведениями, составляющими государственную тайну).

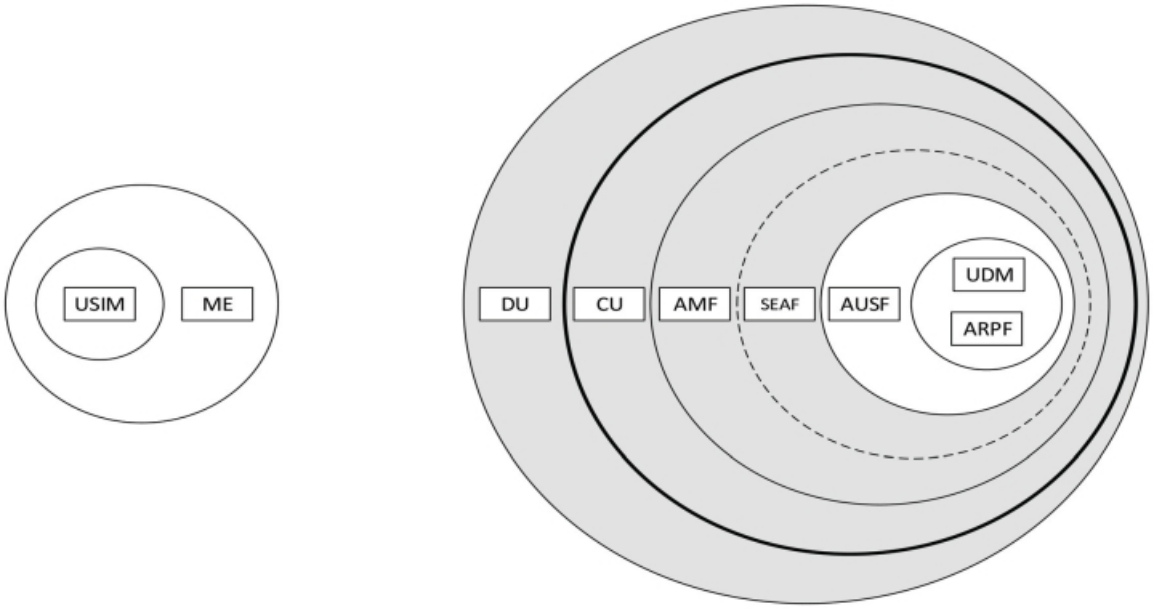
Заказчику нужны результаты научно-исследовательской работы по теме: "Разработка раздела Концепции создания и развития сетей 5G/IMT-2020 в Российской Федерации в части определения принципов и требований обеспечения информационной безопасности сети 5G/IMT-2020, основанных на применении российских криптографических алгоритмов и аппаратных средств, в том числе отечественных USIM-карт с доверенным ПО и ключами, российской системы обеспечения и управления ключами, отечественного доверенного абонентского и сетевого оборудования и ПО, обеспечивающих устойчивость функционирования разрабатываемого оборудования, а также доступность разрабатываемой сети связи".

Из названия НИР следует, что в сетях 5G на территории России предполагается применение российских USIM-карт, абонентского и сетевого оборудования, получившего сертификат соответствия и/или имеющего статус "российского происхождения".

Особенности сетей пятого поколения

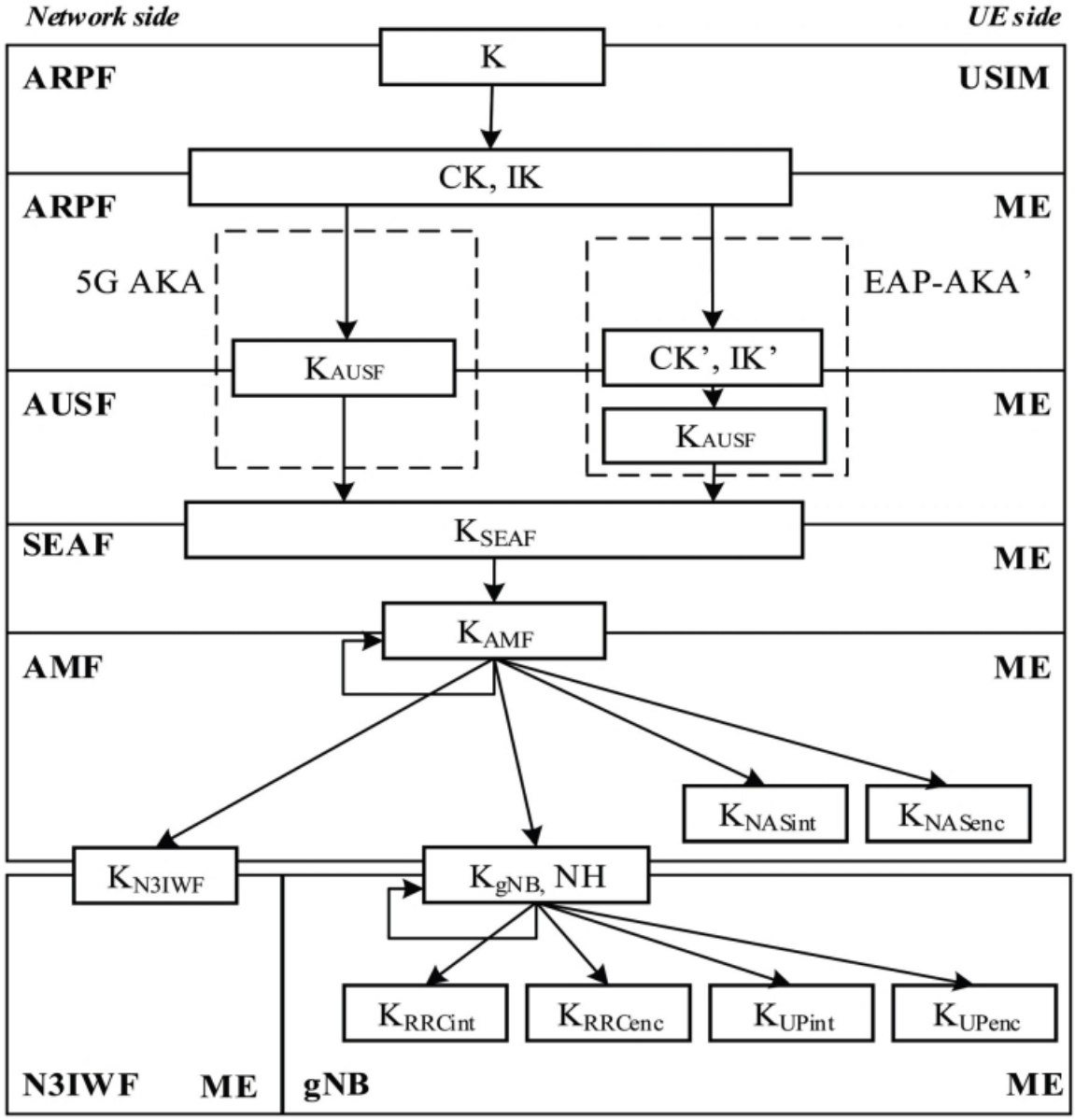
Разработчики стандартов сотовой связи не ограничиваются только вопросами повышения скорости, улучшениями каких-то технических параметров, они серьёзно занимаются вопросами безопасности. Были пересмотрены такие угрозы безопасности как атаки, направленные на радиоинтерфейс, плоскости управления и пользователя, masquerading, replay, bidding down, man-in-the-middle (MITM).

Например, для сотовой сети 5G, функционирующей в соответствии со стандартом 3GPP 5G Phase 1 Release 15, предложена вот такая многослойная доверенная среда:



Universal Subscriber Identity Module (USIM), Mobile Equipment (ME), Access and Mobility Management Function (AMF),
SEcurity Anchor Function (SEAF), Authentication Server Function (AUSF), Repository and Processing Function (ARPF),
Unified Data Management (UDM)

И предусмотрена следующая иерархия ключей:



Extensible Authentication Protocol (EAP), Authentication and Key Agreement (AKA), Cipher Key

(CK), Integrity Key (IK),
Non-3GPP Inter Working Function (N3IWF), gNB - 5G base-station

Большая работа в сфере безопасности будет выполнена на следующем этапе – при разработке 5G Phase 2 (Release 16), завершение и утверждение которой планируется во второй половине 2019 года. Особенностью системы безопасности для решений IoT является необходимость в рамках одной архитектуры обеспечить достаточно высокий уровень защиты как для сценариев массовой работы устройств M2M (mMTC), так и для соединений повышенной надёжности и с очень малой задержкой (URLLC). Если для mMTC характерно очень большое количество устройств, передающих небольшой объём данных, для которых задержка не критична, то для URLLC на первом месте жёсткие требования к пропускной способности, к задержкам и к постоянной доступности сети.

При эксплуатации решений mMTC (massive Machine Type Communication) достаточно небольшой скорости передачи данных объёмом несколько бит (например, температурные датчики, передающие данные раз в час, датчики на сельскохозяйственных животных, фиксирующие событие пару раз за день и другие подобные проекты). При этом устройства mMTC имеют ограничения по энергопитанию (зависимость от ёмкости и состояния аккумулятора), по вычислительным ресурсам и по объёму памяти. Поэтому вряд ли стоит использовать стандартный подход, когда выполняются алгоритмы, рассчитанные на вычислительные операции с многобитовыми ключами без требований по времени выполнения, необходимо также обращать внимание на энергоэффективность алгоритмов и на вычислительные ограничения.

Иные требования для решений URLLC (Ultra-Reliable and Low Latency Communications), где будут востребованы высокие скорости, минимум проблем с энергопитанием и маловероятны существенные ограничения на вычислительные ресурсы. Имеются в виду "подключенные" автомобили, устройства для промышленного IoT (Industrial IoT – IIoT), AR/VR-устройства и т.д. В этом случае, первоочередной задачей становится исключение или минимизация задержек данных при выполнении процедур на различных этапах, предусмотренных в системе безопасности сотовой сети связи.

Учитывая описанные сложности и противоречивые требования к алгоритмам аутентификации и др., удастся ли в сетях 5G продолжить начатое Минкомсвязи внедрение отечественных СКЗИ в сотовой связи?

Изменения для провайдеров

В Минкомсвязи решили, что категории узлов связи в сетях передачи данных необходимо определять по монтированной ёмкости (пропускной способности). В обновлённом варианте приказа от 9 января 2008 года № 1 "Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации" для сетей передачи данных предложено изменить с 1 декабря 2019 года критерии для определения категории узлов связи по защищённости. В настоящее время:

Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. N 1 "Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации"

Зарегистрировано в Минюсте РФ 23 января 2008 г.

Приложение
к Требованиям

Категорирование узлов связи по защищенности

Типы сетей	Категории		
	I	II	III
Сети фиксированной телефонной связи	узлы связи сетей междугородной и международной телефонной связи, сетей зоновой телефонной связи, узлы связи сетей местной телефонной связи с количеством портов более 10000, а также транзитные и оконечно-транзитные узлы связи сетей местной телефонной связи, которые соединяются с узлами обслуживания вызовов экстренных оперативных служб	узлы связи сети местной телефонной связи с количеством портов от 1024 до 10000, за исключением транзитных и оконечно-транзитных узлов связи, которые соединяются с узлами обслуживания вызовов экстренных оперативных служб	узлы связи сети местной телефонной связи с количеством портов до 1024
Сети подвижной радиосвязи, сети подвижной радиотелефонной связи, сети подвижной спутниковой радиосвязи	узлы связи сети подвижной радиосвязи, узлы связи сети подвижной радиотелефонной связи, узлы связи в составе наземных станций сопряжения сети подвижной спутниковой радиосвязи		
Сети передачи данных	международные транзитные узлы связи	транзитные узлы связи	оконечные узлы связи, оконечно-транзитные узлы связи
Сети телеграфной связи	международные узлы связи	междугородние узлы связи	зоновые узлы связи

Источник: http://www.garant.ru/products/ipo/prime/doc/92632/

Изменения с 1 декабря 2019 года:

Приложение № 1
к Требованиям по защите сетей связи от несанкционированного доступа и передаваемой по ним информации, утвержденным приказом Министерства связи и массовых коммуникаций Российской Федерации
от _____ № _____

Категорирование узлов связи по защищенности

Категории / Типы сетей	I	II	III
Сети фиксированной телефонной связи	узлы связи сетей междугородной и международной телефонной связи, сетей зоновой телефонной связи, узлы связи сетей местной телефонной связи с количеством портов более 10000, а также транзитные и оконечно-транзитные узлы связи сетей местной телефонной связи, которые соединяются с узлами обслуживания вызовов экстренных оперативных служб	узлы связи сети местной телефонной связи с количеством портов от 1024 до 10000, за исключением транзитных и оконечно-транзитных узлов связи, которые соединяются с узлами обслуживания вызовов экстренных оперативных служб	узлы связи сети местной телефонной связи с количеством портов до 1024
Сети подвижной радиосвязи, сети подвижной радиотелефонной связи, сети подвижной спутниковой радиосвязи	узлы связи сети подвижной радиосвязи, узлы связи сети подвижной радиотелефонной связи, узлы связи в составе наземных станций сопряжения сети подвижной спутниковой радиосвязи		
Сети передачи данных	узлы сети передачи данных монтированной емкостью свыше 500 Гбит в секунду	узлы сети передачи данных монтированной емкостью свыше 100 Гбит и менее 500 Гбит в секунду	узлы сети передачи данных монтированной емкостью менее 100 Гбит в секунду
Сети телеграфной связи	международные узлы связи	междугородние узлы связи	зоновые узлы связи

Источник: проект приказа по итогам обсуждения http://regulation.gov.ru/projects#npa=76975

---

* Проект приказа Минкомсвязи России "О внесении изменений в Правила применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VI. Правила применения узлов связи с территориально распределенной архитектурой стандартов UMTS и/или GSM 900/1800, утвержденные приказом Министерства связи и массовых коммуникаций Российской Федерации от 27.06.2011 N 160". ID проекта – 02/08/12-17/00076963, Дата создания – 27 декабря 2017 года, ссылка.

** После окончания общественного обсуждения была проведена доработке проекта приказа и из него удалена та часть первоначальной версии, которая относилась к сетям LTE. Оказалось, что для сетей этого стандарта уже внесены требования по применению СКЗИ, сертифицированные ФСБ - подпункты 5 и 6 пункта 15 в "Правилах... " - см. Приказ Минкомсвязи России от 25.06.2018 N 319 "Об утверждении Правил применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VII. Правила применения оборудования коммутации стандарта LTE" (Зарегистрировано в Минюсте России 31.07.2018 N 51741). Данные требования вступают в силу с 1 декабря 2019 года, ссылка.