Международный союз электросвязи

# МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

# X.1811

(04/2021)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность сетей IMT-2020

## Руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность

Рекомендация МСЭ-Т X.1811

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

**СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ**

| | |
|---|---|
| СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ | X.1–X.199 |
| ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ | X.200–X.299 |
| ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ | X.300–X.399 |
| СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ | X.400–X.499 |
| СПРАВОЧНИК | X.500–X.599 |
| ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ | X.600–X.699 |
| УПРАВЛЕНИЕ В ВОС | X.700–X.799 |
| БЕЗОПАСНОСТЬ | X.800–X.849 |
| ПРИЛОЖЕНИЯ ВОС | X.850–X.899 |
| ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА | X.900–X.999 |
| БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ | |
| Общие аспекты безопасности | X.1000–X.1029 |
| Безопасность сетей | X.1030–X.1049 |
| Управление безопасностью | X.1050–X.1069 |
| Телебиометрия | X.1080–X.1099 |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1) | |
| Безопасность многоадресной передачи | X.1100–X.1109 |
| Безопасность домашних сетей | X.1110–X.1119 |
| Безопасность подвижной связи | X.1120–X.1139 |
| Безопасность веб-среды | X.1140–X.1149 |
| Протоколы безопасности (1) | X.1150–X.1159 |
| Безопасность одноранговых сетей | X.1160–X.1169 |
| Безопасность сетевой идентификации | X.1170–X.1179 |
| Безопасность IPTV | X.1180–X.1199 |
| БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА | |
| Кибербезопасность | X.1200–X.1229 |
| Противодействие спаму | X.1230–X.1249 |
| Управление определением идентичности | X.1250–X.1279 |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2) | |
| Связь в чрезвычайных ситуациях | X.1300–X.1309 |
| Безопасность повсеместных сенсорных сетей | X.1310–X.1319 |
| Безопасность "умных" электросетей | X.1330–X.1339 |
| Сертифицированная электронная почта | X.1340–X.1349 |
| Безопасность интернета вещей (IoT) | X.1360–X.1369 |
| Безопасность интеллектуальных транспортных систем (ИТС) | X.1370–X.1389 |
| Безопасность технологии распределения реестра | X.1400–X.1429 |
| Безопасность технологии распределения реестра | X.1430–X.1449 |
| Протоколы безопасности (2) | X.1450–X.1459 |
| ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ | |
| Обзор кибербезопасности | X.1500–X.1519 |
| Обмен информацией об уязвимости/состоянии | X.1520–X.1539 |
| Обмен информацией о событии/инциденте/эвристических правилах | X.1540–X.1549 |
| Обмен информацией о политике | X.1550–X.1559 |
| Эвристические правила и запрос информации | X.1560–X.1569 |
| Идентификация и обнаружение | X.1570–X.1579 |
| Гарантированный обмен | X.1580–X.1589 |
| БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ | |
| Обзор безопасности облачных вычислений | X.1600–X.1601 |
| Проектирование безопасности облачных вычислений | X.1602–X.1639 |
| Передовой опыт и руководящие указания в области облачных вычислений | X.1640–X.1659 |
| Обеспечение безопасности облачных вычислений | X.1660–X.1679 |
| Другие вопросы безопасности облачных вычислений | X.1680–X.1699 |
| КВАНТОВАЯ СВЯЗЬ | |
| Терминология | X.1700–X.1701 |
| Квантовый генератор случайных чисел | X.1702–X.1709 |
| Структура безопасности QKDN | X.1710–X.1711 |
| Проектирование безопасности QKDN | X.1712–X.1719 |
| Методы обеспечения безопасности QKDN | X.1720–X.1729 |
| БЕЗОПАСНОСТЬ ДАННЫХ | |
| Безопасность больших данных | X.1750–X.1759 |
| **БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020** | **X.1800–X.1819** |

*Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.*

**Рекомендация МСЭ-Т X.1811**

# Руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность


**Резюме**

В Рекомендации МСЭ-Т X.1811 определены угрозы, которые квантовые вычисления создают системам Международной подвижной электросвязи-2020 (IMT-2020), на основании оценки уровня безопасности используемых в настоящее время криптографических алгоритмов. В настоящей Рекомендации содержится краткий обзор алгоритмов, обеспечивающих квантовую безопасность, включая алгоритмы как симметричного, так и несимметричного типов, и приведены руководящие указания для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность.



**Хронологическая справка**

| Издание | Рекомендация | Утверждено | Исследовательская комиссия | Уникальный идентификатор* |
|---|---|---|---|---|
| 1.0 | МСЭ-Т X.1811 | 30.04.2021 | 17-я | 11.1002/1000/14454 |

**Ключевые слова**

Алгоритм, квантовый компьютер, несимметричный алгоритм, обеспечивающий квантовую безопасность, симметричный алгоритм, система 5G, система IMT-2020.


* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например, http://handle.itu.int/11.1002/1000/11830-en.

## ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

## ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

## ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу http://www.itu.int/ITU-T/ipr/.

**СОДЕРЖАНИЕ**

**Стр.**

## Введение

Система Международной подвижной электросвязи-2020 (IMT-2020) обещает поддерживать широкий спектр услуг с различными требованиями к их характеристикам в целях построения полностью соединенного общества. Для достижения этой непростой цели в системе IMT-2020 был разработан ряд инновационных технологий, таких как нарезка (сегментирование) сети, сеть с программируемыми параметрами, виртуализированная сетевая функция и разделение на центральный и распределенные блоки (CU/DU). Меры безопасности имеют основополагающее значение для обеспечения нормальной работы системы IMT-2020. Помимо симметричных в системе IMT-2020 используются несимметричные криптографические алгоритмы.

Большой квантовый компьютер создает проблемы, связанные с безопасностью, для широко используемых в настоящее время симметричных и несимметричных криптографических алгоритмов. Последние больше не гарантируют безопасности в эпоху квантовых вычислений. А для того чтобы симметричные криптографические алгоритмы могли противостоять атакам на основе квантовых вычислений, длина их ключей должна быть удвоена. По этим причинам в системе IMT-2020 крайне желательно применять криптографические алгоритмы, обеспечивающие квантовую безопасность.

В настоящей Рекомендации содержится краткое описание системы IMT-2020 и ее архитектуры безопасности. Проводится оценка угроз для систем IMT-2020, связанных с применением квантовых компьютеров. Дается краткий обзор алгоритмов, обеспечивающих квантовую безопасность, но их детали в настоящей Рекомендации не рассматриваются. Руководящие указания по безопасности будут включены в Рекомендацию высокого уровня по адаптации алгоритмов, обеспечивающих квантовую безопасность, к системам IMT-2020. Настоящая Рекомендация содержит руководящие указания по применению в системе IMT-2020 симметричных и несимметричных алгоритмов, обеспечивающих квантовую безопасность, а также по согласованию уровней безопасности между симметричными и несимметричными алгоритмами, обеспечивающими квантовую безопасность.

# Рекомендация МСЭ-Т X.1811

## Руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность

### 1 Сфера применения

В настоящей Рекомендации содержатся:

– введение в архитектуру безопасности систем Международной подвижной электросвязи – 2020 (IMT-2020);

– оценка безопасности систем IMT-2020 при наличии коммерческих квантовых компьютеров;

– описание применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность.

### 2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса Рекомендации.

[ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 год), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ*

[ITU-T X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*

### 3 Определения

#### 3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

**3.1.1 Аутентификация (authentication)** [b-ITU-T X.2014] – свойство, посредством которого с требуемой гарантией устанавливается верная идентичность объекта или участвующей стороны. Стороной, проходящей аутентификацию, может являться пользователь, абонент, оператор домашней сети или обслуживающая сеть.

**3.1.2 Протокол аутентификации (authentication protocol)** [b-ITU-T X.1254] – определенная последовательность сообщений между объектом и верификатором, которая позволяет верификатору выполнить аутентификацию объекта.

**3.1.3 Авторизация (authorization)** [b-ISO 7498-2] – предоставление прав, которое включает предоставление доступа на основании прав доступа.

**3.1.4 Готовность (availability)** [ITU-T X.800] – свойство быть доступным и годным к использованию по запросу имеющего полномочия объекта.

**3.1.5 Регистрационные данные (credential)** [b-ITU-T X.1252] – набор данных, представляемых как доказательство утверждаемой идентичности и/или прав.

**3.1.6 Конфиденциальность (confidentiality)** [ITU-T X.800] – свойство, защищающее информацию от доступа к ней или ее раскрытия неуполномоченными лицами, устройствами или процессами.

**3.1.7 Целостность данных (data integrity)** [ITU-T X.800] – показатель того, что данные не были изменены или разрушены несанкционированным способом.

**3.1.8 Неприкосновенность частной жизни (privacy)** [ITU-T X.800] – право частного лица контролировать или воздействовать на то, какая касающаяся его информация может быть собрана и сохранена, а также кем и кому эта информация может быть открыта.

**3.1.9 Иерархия ключей (key hierarchy)** [b-ITU X.1196] – древовидная структура, отражающая взаимосвязь между разными ключами. В иерархии ключей узел соответствует ключу, используемому для получения ключей, представленных узлами-потомками. Ключ может иметь только одного предшественника, но несколько узлов-потомков.

**3.1.10 Виртуализация сетевых функций (network function virtualization; NFV)** [b-ISO/IEC TR 22417] – технология, которая позволяет создавать логически изолированные участки сети в общих физических сетях, так чтобы в них могли одновременно сосуществовать разнородные группы из нескольких виртуальных сетей.

### 3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

## 4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

| | | |
|---|---|---|
| 4G | fourth Generation | Четвертое поколение |
| AES | Advanced Encryption Standard | Усовершенствованный стандарт шифрования |
| AES-CBC | Advanced Encryption Standard-Cipher Blocker Chaining | Усовершенствованный стандарт шифрования – сцепление шифрованных блоков |
| AES-GCM | Advanced Encryption Standard-Galois Counter Mode | Усовершенствованный стандарт шифрования – режим счетчика Галуа |
| AES-GMAC | Advanced Encryption Standard-Galois Message Authentication Code | Усовершенствованный стандарт шифрования – код аутентификации сообщений Галуа |
| AF | Application Function | Функция приложения |
| AKA | Authentication and Key Agreement | Соглашение об аутентификации и ключах; аутентификация и согласование ключей |
| AMF | Access and Mobility management Function | Функция управления доступом и мобильностью |
| API | Application Programming Interface | Интерфейс прикладного программирования |
| ARPF | Authentication credential Repository and Processing Function | Хранилище и функция обработки регистрационных данных |
| AS | Access Stratum | Уровень доступа |
| AUSF | Authentication Server Function | Функция сервера аутентификации |
| AV | Authentication Vector | Вектор аутентификации |
| CEK | Content Encryption Key | Ключ шифрования контента |
| CM | Configuration Management | Управление конфигурацией |
| CP | Control Plane | Плоскость управления |
| CU/DU | Central Unit/Distributed Unit | Центральный блок/распределенный блок |
| DH | Diffie-Hellman | Алгоритм Диффи – Хеллмана |

| | | |
|---|---|---|
| DHE | Diffie-Hellman Ephemeral | Временный ключ Диффи – Хеллмана |
| DNSSec | Domain Name System Security extensions | Расширения безопасности системы доменных имен |
| DSA | Digital Signature Algorithm | Алгоритм цифровой подписи |
| DTLS | Datagram Transport Layer Security | Протокол дейтаграмм безопасности транспортного уровня |
| EAP | Extensible Authentication Protocol | Расширяемый протокол аутентификации |
| ECC | Elliptic-Curve Cryptography | Шифрование методом эллиптических кривых |
| ECDH | Elliptic Curve Diffie-Hellman | Протокол Диффи – Хеллмана на эллиптических кривых |
| ECDHE | Elliptic Curve Diffie-Hellman Ephemeral | Временный ключ протокола Диффи – Хеллмана на эллиптических кривых |
| ECDLP | Elliptic Curve Discrete-Log Problem | Задача дискретного логарифмирования на эллиптической кривой |
| ECDSA | Elliptic Curve Digital Signature Algorithm | Алгоритм цифровой подписи на основе эллиптических кривых |
| ECIES | Elliptic Curve Integrated Encryption Scheme | Объединенный алгоритм шифрования на основе эллиптических кривых |
| ECP | Extended Cutting Plane | Расширенная секущая плоскость |
| eMBB | enhanced Mobile Broadband | Усовершенствованная подвижная широкополосная связь |
| ESP | Encapsulating Security Payload | Инкапсуляция полезной нагрузки безопасности |
| FM | Fault Management | Управление ошибками |
| GKDF | Generic Key Derivation Function | Функция выработки общего ключа |
| gNB | NR Node B | Узел B NR |
| GUTI | Globally Unique Temporary Identifier | Глобальный временный уникальный идентификатор |
| HMAC | Hash-based Message Authentication Code | Хеш-код аутентификации сообщений |
| HKDF | HMAC-based Extract-and-Expand Key Derivation Function | Функция выработки ключа извлечения и расширения на основе HMAC |
| ICV | Integrity Check Value | Значение проверки целостности |
| IPsec | Internet Protocol Security | Безопасность протокола Интернет |
| IKE | Internet Key Exchange | Протокол обмена ключами по интернету |
| IKEv2 | Internet Key Exchange version 2 | Протокол обмена ключами по интернету версии 2 |
| IMT-2020 | International Mobile Telecommunications-2020 | Международная подвижная электросвязь – 2020 |
| IP | Internet Protocol | Протокол Интернет |
| IPX | IP exchange | Обмен трафиком интернета |
| JOSE | Javascript Object Signing And Encryption | Подпись и шифрование объектов JavaScript |

| | | |
|---|---|---|
| JSON | JavaScript Object Notation | Нотация объектов JavaScript |
| JWE | JSON Web Encryption | Веб-шифрование JSON |
| JWS | JSON Web Signature | Веб-подпись JSON |
| KDF | Key Derivation Function | Функция выработки ключей |
| KEM | Key Encapsulation Mechanism | Механизм инкапсуляции ключей |
| LTE | Long-Term Evolution | Долгосрочное развитие |
| LWE | Learning With Errors | Обучение с ошибками |
| MAC | Message Authentication Code | Код аутентификации сообщений |
| mIoT | massive Internet of Things | Массовый интернет вещей |
| mMTC | massive Machine-Type Communication | Массовая связь машинного типа |
| MNO | Mobile Network Operator | Оператор сети подвижной связи |
| MODP | Modular exponential | Модульная экспонента |
| MPLS | Multiprotocol Label Switching | Многопротокольная коммутация по меткам |
| N3IWF | Non-3GPP Interworking Function | Функция взаимодействия нестандарта 3GPP (не-3GPP) |
| NAS | Non-Access Stratum | Уровень, не связанный с предоставлением доступа |
| NDS | Network Domain Security | Безопасность сетевого домена |
| NEF | Network Exposure Function | Функция представления сети |
| NF | Network Function | Сетевая функция |
| NFV | Network Function Virtualization | Виртуализация сетевых функций |
| NFVI | Network Function Virtualization Infrastructure | Инфраструктура виртуализации сетевых функций |
| NG-RAN | Next Generation-Radio Access Network | Сети радиодоступа последующих поколений |
| NP | Non-deterministic Polynomial time | Недетерминированное полиномиальное время |
| NRF | NF Repository Function | Функция репозитория NF |
| NSSF | Network Slice Selection Function | Функция выбора сетевого сегмента |
| NTRU | *N*th degree Truncated Polynomial Ring | Усеченное кольцо многочленов *N*-й степени |
| PCF | Policy Control Function | Функция управления политикой |
| PDCP | Packet Data Convergence Protocol | Протокол сходимости пакетных данных |
| PKI | Public-Key Infrastructure | Инфраструктура криптографической защиты с открытым ключом |
| PKE | Public-Key Encryption | Шифрование с открытым ключом |
| PM | Performance Management | Управление рабочими характеристиками |
| PRF | Pseudo-Random Function | Псевдослучайная функция |
| PSK | Pre-Shared Key | Предварительно распространенный ключ |

| | | |
|---|---|---|
| RLC | Radio Link Control | Управление радиоканалом |
| R-LWE | Ring Learning With Errors | Обучение с ошибками в кольце |
| RRC | Radio Resource Control | Управление радиоресурсами |
| RSA | Rivest, Shamir and Adleman | Алгоритм Райвеста – Шамира – Адлемана |
| PLMN | Public Land Mobile Network | Сухопутная подвижная сеть общего пользования |
| PQC | Post-Quantum Cryptography | Постквантовая криптография |
| SBA | Service-Based Architecture | Сервис-ориентированная архитектура; архитектура, ориентированная на услуги |
| SDAP | Service Data Adaptation Protocol | Протокол адаптации служебных данных |
| SDN | Software-Defined Network | Сеть с программируемыми параметрами |
| SEAF | Security Anchor Function | Якорная функция безопасности |
| SEPP | Security Edge Protection Proxy | Периферийный прокси-сервер безопасности |
| SHA | Secure Hash Algorithm | Защищенный алгоритм хеширования |
| SIDF | Subscription Identifier De-concealing Function | Функция извлечения идентификатора абонента |
| SIDH | Supersingular-Isogeny Diffie–Hellman | Алгоритм Диффи – Хеллмана с использованием суперсингулярных изогений |
| SIKE | Supersingular Isogeny Key Encapsulation | Инкапсуляция ключей с использованием суперсингулярных изогений |
| SMF | Session Management Function | Функция управления сеансом |
| SSH | Secure Shell | Защищенный командный процессор |
| SUCI | Subscription Concealed Identifier | Скрытый идентификатор абонента |
| SUPI | Subscription Permanent Identifier | Постоянный идентификатор абонента |
| SVP | Shortest Vector Problem | Задача поиска кратчайшего вектора |
| TLS | Transport Layer Security | Безопасность транспортного уровня |
| TM | Trace Management | Управление трассировкой |
| UDM | Unified Data Management | Единое управление данными |
| UDR | User Data Repository | Хранилище пользовательских данных |
| UE | User Equipment | Оборудование пользователя; пользовательское оборудование |
| UOV | Unbalanced Oil and Vinegar | "Несбалансированная схема масла и уксуса" |
| UP | User Plane | Плоскость пользователя |
| UPF | User Plane Function | Функция плоскости пользователя |
| URLLC | Ultra-Reliable and Low-Latency Communication | Сверхнадежная связь с короткой задержкой |
| USIM | Universal Subscriber Identity Module | Универсальный модуль идентификации абонента |

| | | |
|---|---|---|
| VNF | Virtual Network Function | Функция виртуальной сети |
| WLAN | Wireless Local Area Network | Беспроводная локальная сеть |
| XMSS | extended Merkle Signature Scheme | Расширенная схема подписи Меркла |

## 5 Соглашения

В настоящей Рекомендации:

ключевые слова "**требуется, чтобы**" обозначают требование, которое должно строго соблюдаться и от которого не допускается отклонений, если должно быть заявлено соответствие данной Рекомендации;

ключевое слово "**рекомендуется**" обозначает требование, которое рекомендовано, но не обязательно требуется. Поэтому для заявления о соответствии это требование не обязательно;

ключевые слова "**запрещено, чтобы**" обозначают требование, которое должно строго соблюдаться и от которого не допускается отклонений, если должно быть заявлено соответствие данной Рекомендации;

ключевые слова "**необязательно можно**" обозначают необязательное требование, которое допустимо, не имеет рекомендательного значения. Этот термин не предназначен для утверждения, что реализация поставщика должна обеспечивать этот вариант, а функцию может необязательно предоставлять оператор сети/поставщик услуг. Наоборот, это значит, что поставщик может необязательно предоставлять эту функцию и тем не менее заявлять о соответствии техническим условиям.

## 6 Обзор

Технология подвижной связи IMT-2020 призвана удовлетворять потребностям бизнеса в 2020 году и в дальнейшем. Архитектура безопасности играет ключевую роль в обеспечении нормальной работы сети IMT-2020. В сетях четвертого поколения/долгосрочного развития (4G/LTE) для защиты сигнализации и пользовательских данных применяются только симметричные алгоритмы. В системах IMT-2020 в дополнение к ним вводятся несимметричные алгоритмы для обеспечения защиты не только идентификаторов абонентов, но и связи между операторами сетей подвижной связи (MNO).

Недавно (по состоянию на сентябрь 2020 года) компания IBM анонсировала 50-кубитовый квантовый компьютер [b-QC1]. Этот прорыв нарушил первоначальные ожидания того, что мощные квантовые компьютеры появятся на рынке через 20 лет. Согласно приведенной в новом отчете [b-QC2] оценке, реалистичный срок их появления составит 10 лет.

Безопасность криптографических алгоритмов с открытым ключом зависит от сложности вычислительных задач, таких как разложение на простые множители большого целого числа или задача дискретного логарифмирования по различным группам. Как установлено, квантовые компьютеры способны эффективно решать каждую из этих задач [b-Shor 1997], что сделает все криптосистемы с открытым ключом, основанные на таких задачах, бессильными. Таким образом, достаточно мощный квантовый компьютер поставит под угрозу многие формы современных криптосистем, такие как обмен ключами, шифрование и цифровая аутентификация.

Квантовые компьютеры повлияют на уровень безопасности симметричных и несимметричных алгоритмов в разной степени. Стойкость симметричных криптографических алгоритмов уменьшится вдвое; например, для усовершенствованного стандарта шифрования (AES) с 128-битовыми ключами, обеспечивающего стойкость 128 битов, она снизится до 64 битов, а многие широко используемые несимметричные алгоритмы, такие как алгоритм Райвеста – Шамира – Адлемана (RSA), алгоритм цифровой подписи (DSA) и шифрование методом эллиптических кривых (ECC), не будут обеспечивать никакой защиты.

Система IMT-2020 предназначена для предоставления широкого спектра услуг с различными требованиями к их характеристикам. Услуги, предоставляемые в сетях IMT-2020, можно подразделить на услуги усовершенствованной подвижной широкополосной связи (eMBB), массового интернета вещей (mIoT) и сверхнадежной связи с короткой задержкой (URLLC).

Система IMT-2020 вводит ряд инновационных технологий, таких как нарезка сети, виртуализация сетевых функций (NFV), сеть с программируемыми параметрами (SDN) и сервис-ориентированная

архитектура (SBA). Эти технологии делают систему IMT-2020 гибкой платформой, позволяющей создавать новые бизнес-модели и интегрировать вертикальные отрасли. В то же время они значительно усложняют архитектуру безопасности системы IMT-2020 по сравнению с сетями подвижной связи предыдущих поколений.

Крайне необходимо изучить методы защиты связи в системах IMT-2020 с использованием алгоритмов**,** обеспечивающих квантовую безопасность. Это обусловлено вероятностью того, что в течение жизненного цикла систем IMT-2020 станут доступны коммерческие квантовые компьютеры. В настоящее время длина ключа симметричных алгоритмов, определенная для систем IMT-2020, составляет 128 битов. В рамках Проекта партнерства 3-го поколения (3GPP) только что был инициирован вопрос для исследования, посвященный применению в системах IMT-2020 симметричных алгоритмов с длиной ключа 256 битов [b-3GPP TR 33.841]. Однако до сих пор ни одна организация не занимается изучением возможности применения к системам IMT-2020 несимметричных алгоритмов**,** обеспечивающих квантовую безопасность. При использовании в системах IMT-2020 криптографических алгоритмов**,** обеспечивающих квантовую безопасность, требуется некоторая адаптация, поскольку длина их ключей больше длины ключей, принятой в классической криптографии. Более того, необходимо изучить, как в системах IMT-2020 смогут сосуществовать ключи разного размера, поскольку невозможно в одночасье заменить все классические алгоритмы алгоритмами, обеспечивающими квантовую безопасность. Возможность перехода на криптографию**,** обеспечивающую квантовую безопасность, в системах IMT-2020 следует рассмотреть как можно раньше, чтобы любая информация, которая впоследствии будет раскрыта с применением квантового криптоанализа, не была конфиденциальной.

В настоящей Рекомендации приводится оценка угроз для систем IMT-2020 со стороны квантовых компьютеров. Дается краткий обзор алгоритмов, обеспечивающих квантовую безопасность, но их детали в настоящей Рекомендации не рассматриваются. В руководящих указаниях по безопасности высокого уровня рекомендуется адаптировать алгоритмы**,** обеспечивающие квантовую безопасность, к системам IMT-2020. Настоящая Рекомендация содержит всеобъемлющие руководящие указания по применению в системах IMT-2020 симметричных и несимметричных алгоритмов, обеспечивающих квантовую безопасность, а также по согласованию уровней безопасности между симметричными и несимметричными алгоритмами, обеспечивающими квантовую безопасность.

## 7 Введение в компоненты защиты систем IMT-2020

В данном разделе представлена базовая информация о компонентах защиты систем IMT-2020, указанных в документах МСЭ-Т, 3GPP, ETSI, IETF и т. д.

Система связи должна быть способна предоставлять некоторые из следующих услуг обеспечения безопасности системы или передачи данных [ITU-T X.800]: управление доступом (авторизация), аутентификация, неприкосновенность частной жизни, конфиденциальность, целостность данных, невозможность отказа от авторства и готовность.

Услуги безопасности могут обеспечиваться с использованием криптографических или некриптографических механизмов. В настоящей Рекомендации основное внимание уделяется первому виду механизмов, поскольку в ней изучается применение квантовых криптографических алгоритмов в системах IMT-2020.

В соответствии с архитектурой систем IMT-2020G, представленной в Дополнении I, архитектуру безопасности системы IMT-2020 можно описать на трех уровнях: инфраструктуры, сети и плоскости управления.

### 7.1 Безопасность уровня инфраструктуры

Уровень инфраструктуры служит общей основой для поддержки верхнего уровня в системе IMT-2020, в который входят SDN и уровень инфраструктуры виртуализации сетевых функций (NFVI).

#### 7.1.1 Безопасность SDN

Для доставки данных в сети IMT-2020 используется технология SDN вследствие обеспечиваемого ею динамического и гибкого управления потоками трафика. Архитектура безопасности SDN описана в [ITU-T X.1038] и упрощенно иллюстрируется на рисунке 1.

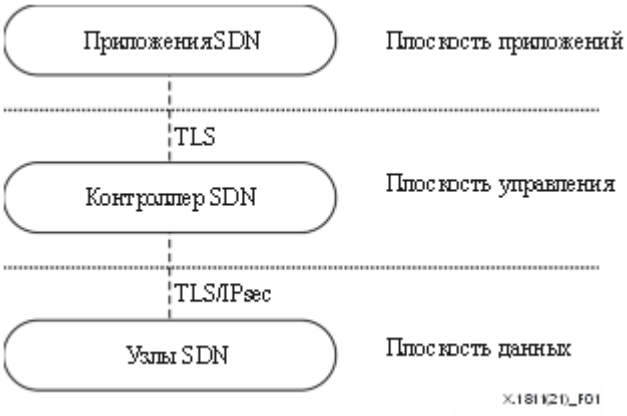


**Рисунок 1 – Архитектура безопасности SDN**

В [ITU-T X.1038] даны следующие рекомендации, касающиеся криптографических алгоритмов и протоколов.

В интерфейсе между приложением SDN и контроллером SDN рекомендуется применять протокол безопасности транспортного уровня (TLS) [b-IETF RFC 5246]. На основе TLS приложение SDN и контроллер SDN аутентифицируют друг друга и согласовывают сеансовый ключ; кроме того, обеспечивается конфиденциальность и целостность данных, передаваемых по интерфейсу управления приложениями.

В интерфейсе между контроллером SDN и узлом SDN рекомендуется применять протокол TLS [b-IETF RFC 5246] или протоколы безопасности протокола Интернет (IPsec) ([b-IETF RFC 4301], [b-IETF RFC 4303], [b-IETF RFC 4835]). На основе TLS или IPsec узел SDN и контроллер SDN аутентифицируют друг друга и согласовывают сеансовый ключ; кроме того, обеспечивается конфиденциальность и целостность данных, передаваемых по интерфейсу управления узлами.

Механизмы аутентификации могут быть основаны либо на предварительно распространенном ключе (PSK) [b-IETF RFC 4279], [b-IETF RFC 4306], либо на сертификате [b-IETF RFC 4306] и [b-IETF RFC 5246]. При аутентификации на основе сертификата можно применять либо RSA [b-ONF TR-511], либо алгоритмы цифровой подписи. Для согласования общего ключа между двумя объектами в контексте TLS или IPsec может применяться протокол обмена ключами на основе алгоритма Диффи – Хеллмана (DH) или алгоритма Диффи – Хеллмана на эллиптических кривых (ECDH).

Криптографическими алгоритмами, используемыми для шифрования данных, могут быть AES [b-NIST FIPS 197], Blowfish [b-Schneier] или 3DES [b-NIST SP 800-67]. Для механизмов обеспечения целостности данных могут применяться криптографические алгоритмы на основе кода аутентификации сообщений (MAC) [b-IETF RFC 2104], хеш-кода аутентификации сообщений (HMAC) [b-IETF RFC 2104] или цифровой подписи [b-NIST FIPS 186-4].

### 7.1.2 Безопасность уровня NFVI

Уровень NFVI, структура которого представлена на рисунке 2, поддерживает выполнение функций виртуальных сетей (VNF).

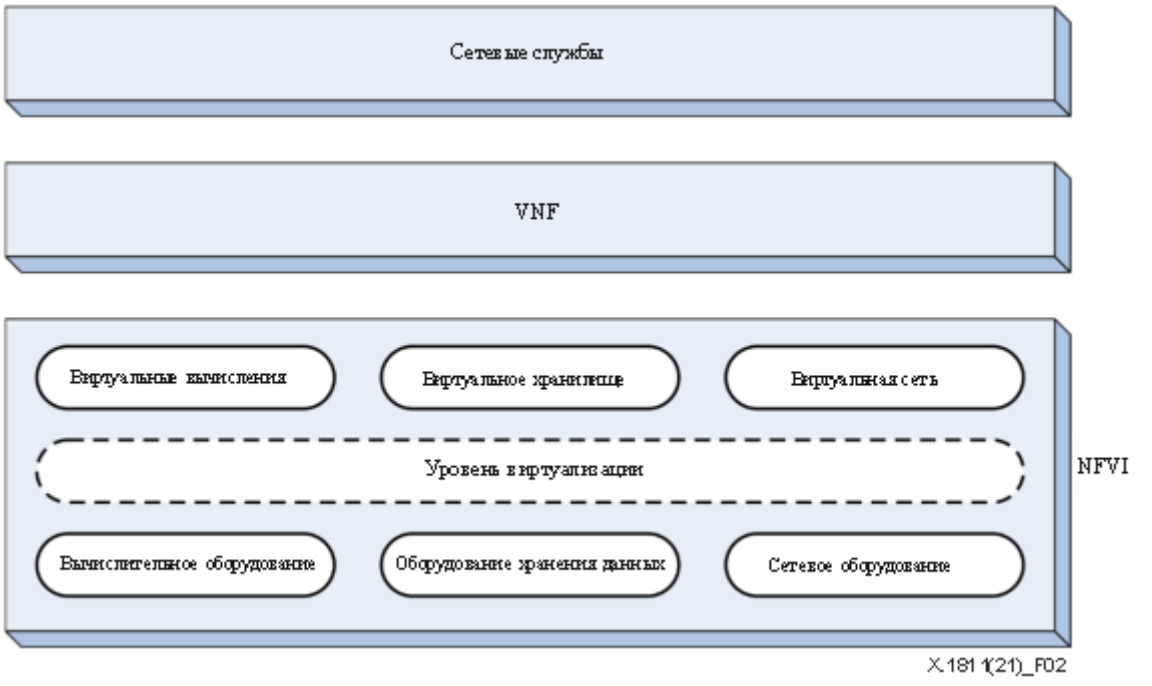


**Рисунок 2 – Структура NFVI (на основе рисунка 1 из [b-ETSI GS NFV 002])**

Согласно [b-ETSI GS NFV-SEC 012] уровень NFVI должен поддерживать следующие функции безопасности для обеспечения защиты VNF, работающих поверх него: безопасное ведение журнала событий; управление доступом и ограничениями на уровне операционной системы; физические элементы управления и сигнализации; элементы управления аутентификацией; элементы управления доступом; безопасность связи; аттестация; аппаратно-опосредованные анклавы исполнения; аппаратный корень доверия; самошифрующееся хранилище данных; прямой доступ к памяти; модули безопасности оборудования; а также защита и проверка целостности программного обеспечения. Для этого NFVI должна реализовывать следующие криптографические алгоритмы [b-ETSI GS NFV-SEC 012]:

1) алгоритмы хеширования: SHA-256, SHA-384, AES128-GMAC, HMAC-SHA128, HMAC-SHA256, HMAC-SHA384;
2) алгоритмы шифрования: AES-CBC-128, AES-GCM-128 (16-октетное значение проверки целостности (ICV)), AES-CBC-256, AES-GCM-256 (16-октетное ICV);
3) алгоритмы цифровой подписи: RSA 2048, RSA 3072, RSA 4096, ECDSA-256 (secp256r1), ECDSA-384 (secp384r1);
4) инфраструктура криптографической защиты с открытым ключом (PKI): RSA 2048, RSA 3072, RSA 4096, id-ecPublicKey (secp256r1);
5) обмен ключами: группа 14 DH (2048-битовая модульная экспонента (MODP)), группа 19 DH (256-битовая группа случайной расширенной секущей плоскости (ECP)), группа 20 DH (384-битовая группа случайной ECP), временный ключ протокола Диффи – Хеллмана на эллиптических кривых (ECDHE) secp256r1 (P-256), группы на основе временных ключей Диффи – Хеллмана (DHE) длиной не менее 2048 битов;
6) псевдослучайная функция (PRF): PRF-HMAC-SHA2-256, PRF-HMAC-SHA2-384.

### 7.2 Безопасность сетевого уровня

#### 7.2.1 Безопасность сети доступа

Безопасность сети доступа [b-3GPP TS 33.501] призвана обеспечить возможность того, чтобы аутентифицированное пользовательское оборудование (UE) получало доступ к сети IMT-2020; связь между UE и сетью IMT-2020 может быть защищена тем способом, который соответствует политике безопасности MNO.

Архитектура безопасности сети доступа IMT-2020, представленная на рисунке 3, может быть описана следующим образом. UE пытается получить доступ к сети с помощью временно присвоенного идентификатора или скрытого постоянного идентификатора, что приводит к активизации протокола соглашения об аутентификации и ключах (AKA). UE и сеть производят взаимную аутентификацию и согласовывают сеансовый ключ, выполняя протокол AKA. UE и сеть получают набор ключей на основе сеансового ключа. Основанная на этих ключах защита целостности и защита от атак повторением сигнальных сообщений уровня, не связанного с предоставлением доступа (NAS), которыми обмениваются UE и функция управления доступом и мобильностью (AMF), является обязательной, а защита их конфиденциальности – факультативной; защита целостности и защита от атак повторением сигнальных сообщений уровня доступа (AS), которыми обмениваются UE и узел B NR (gNB), также являются обязательными, а защита их конфиденциальности – факультативной. Защита конфиденциальности и целостности пользовательских данных в плоскости пользователя (UP) между UE и gNB факультативна. Защита связи между UE и функцией взаимодействия нестандарта 3GPP (N3IWF) в случае не-3GPP-доступа обеспечивается с использованием туннеля IPsec. Поскольку gNB-DU и gNB-CU могут быть установлены в разных местах, защита интерфейса F1 между ними обеспечивается путем применения протокола безопасности сетевого домена/протокола Интернет (NDS/IP). Защита интерфейса E1 между gNB-CU-CP и gNB-CU-UP также основывается на NDS/IP. Транзитная сеть, соединяющая gNB с базовой сетью, защищается с помощью NDS/IP, если в транзитной сети отсутствует физическая защита. Поскольку функция плоскости пользователя (UPF) может применяться на периферии сети, защита связи между UPF и функцией управления сеансом (SMF) также осуществляется с помощью NDS/IP. В отношении архитектуры безопасности сети доступа кратко рассматриваются следующие службы или функции безопасности:

– неприкосновенность частной жизни абонента;
– аутентификация;
– иерархия ключей;
– безопасность сигнализации NAS, сигнализации AS и пользовательских данных;
– NDS/IP;
– безопасность не-3GPP-доступа.

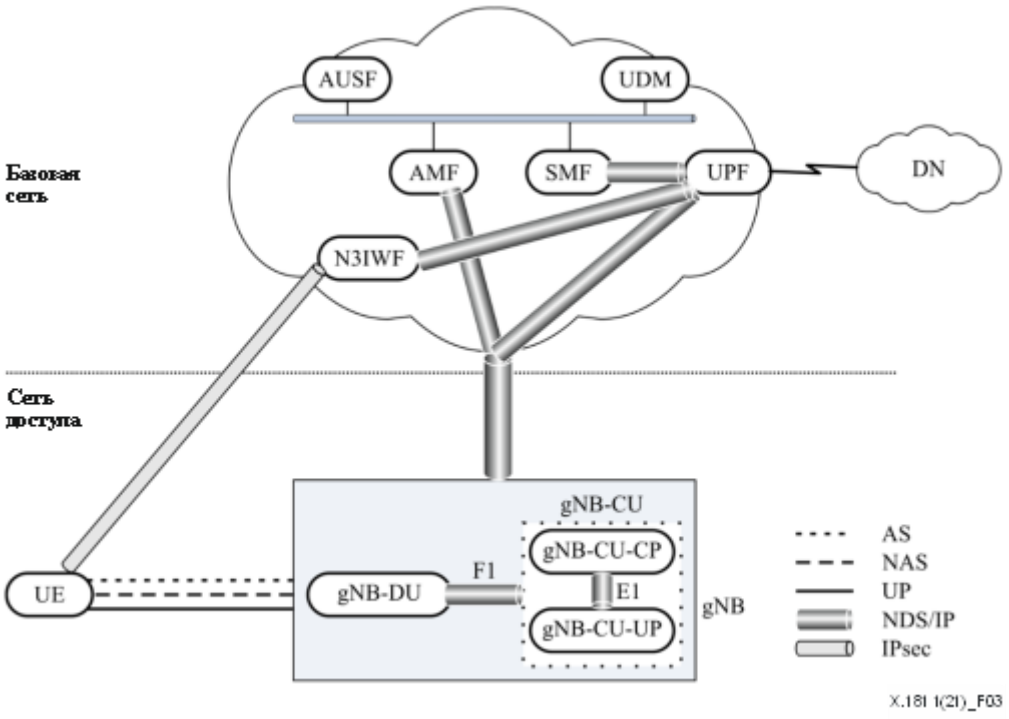


**Рисунок 3 – Архитектура безопасности сети доступа**

#### 7.2.1.1 Неприкосновенность частной жизни абонента

В системе IMT-2020 пользовательскому оборудованию (UE) присваивается глобальный постоянный уникальный идентификатор абонента (SUPI), который передается в универсальный модуль идентификации абонента USIM и модуль единого управления данными/хранилище пользовательских данных (UDM/UDR). При применении USIM IMT-2020 идентификатор SUPI никогда не передается в открытом виде по радиоинтерфейсу. Для начального доступа UE генерирует скрытый идентификатор абонента (SUCI) и передает его в UDM/ARPF (модуль единого управления данными/хранилище и функция обработки регистрационных данных), как показано на рисунке 4. По получении SUCI функция извлечения идентификатора абонента (SIDF), которая находится в модуле ARPF/UDM, извлекает SUPI из SUCI. На основе SUPI модуль UDM/ARPF выбирает метод аутентификации в соответствии с данными абонента.

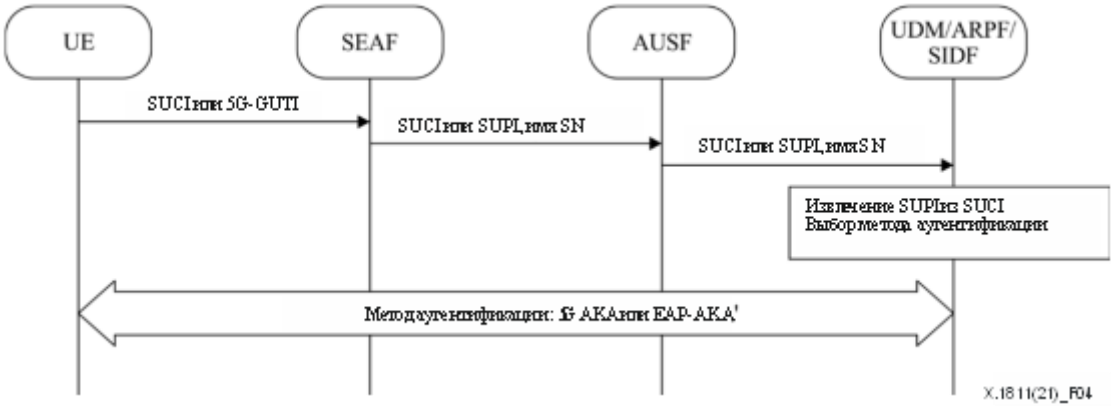


**Рисунок 4 – Начальная процедура аутентификации и выбор метода аутентификации (на основе рисунка 6.1.2-1 из [b-3GPP TS 33.501])**

Идентификатор SUCI состоит из открытой и зашифрованной частей. Первая содержит код страны в системе подвижной связи и код сети подвижной связи в качестве информации, относящейся к домашней сети, для маршрутизации SUCI в целевой модуль UDM/ARPF. Вторая содержит конфиденциальную информацию абонента, а именно идентификационный номер абонента подвижной связи, зашифрованный с использованием объединенного алгоритма шифрования на основе эллиптических кривых (ECIES). Открытый ключ домашней сети надежно передается соответственно в USIM и SIDF. Принцип ECIES заключается в том, что UE и сеть применяют собственный секретный ключ и открытый ключ партнера для согласования общих ключей с помощью механизма ECDH. На основе общих ключей обеспечивается защита конфиденциальности и целостности данных с использованием соответственно симметричных алгоритмов шифрования и алгоритмов MAC. В соответствии с профилями, указанными в [b-3GPP TS 33.501], механизмы ECDH (X25519, примитив DH с кофактором эллиптической кривой) используются для создания общих ключей, а AES-128 в режиме счетчика и HMAC-SHA-256 используются для обеспечения соответственно конфиденциальности и целостности данных.

После инициирования процедуры аутентификации пользовательскому оборудованию (UE) безопасным образом присваивается глобальный временный уникальный идентификатор IMT-2020 (5G-GUTI), чтобы скрыть SUPI в ходе последующей процедуры аутентификации.

#### 7.2.1.2 Аутентификация

В системе IMT-2020 применяются два вида протокола AKA для взаимной аутентификации между UE и сетью и для создания сеансового ключа $K_{SEAF}$, а именно 5G-AKA и расширяемый протокол аутентификации – соглашение об аутентификации и ключах (EAP-AKA'). Последний может использоваться для 3GPP-доступа и не-3GPP-доступа. По сравнению с протоколами сетей 4G протоколы аутентификации сети 5G обеспечивают улучшенный контроль в домашней сети, снижая вероятность мошенничества со стороны сети роуминга. В случае EAP-AKA' проверка идентичности

UE на стороне сети выполняется в функции сервера аутентификации (AUSF) домашней сети. В случае 5G-AKA, хотя проверка идентичности UE на стороне сети выполняется в якорной функции безопасности (SEAF) сети роуминга, AUSF домашней сети проверяет подтверждение аутентификации во время каждой процедуры аутентификации.

В процедуре аутентификации для генерирования вектора аутентификации (AV) и ответа аутентификации используется набор алгоритмов создания ключей (*f*1, *f*1*, *f*2, *f*3, *f*4, *f*5 и *f*5*). Для этого имеются два вида наборов алгоритмов. Один из них называется набором алгоритмов MILENAGE [b-ETSI 135 205], в котором за основу рекомендуется принять AES-128. Другой называется TUAK [b-ETSI 135 231], в котором за основу принята функция криптографической губки Keccak [b-Bertoni] с размером входного ключа 128 или 256 битов. Следует отметить, что на практике набор алгоритмов MILENAGE применяется более широко, чем TUAK.

### 7.2.1.3 Иерархия ключей

Опираясь на корневой ключ K, UE и сеть выполняют взаимную аутентификацию и генерируют сеансовый ключ $K_{SEAF}$, который служит якорем для ключей ($K_{N3IWF}$, $K_{NASint}$, $K_{NASenc}$, $K_{RRCint}$, $K_{RRCenc}$, $K_{UPint}$, $K_{UPenc}$), используемых для обеспечения безопасности связи между UE и сетью, как показано на рисунке 5.

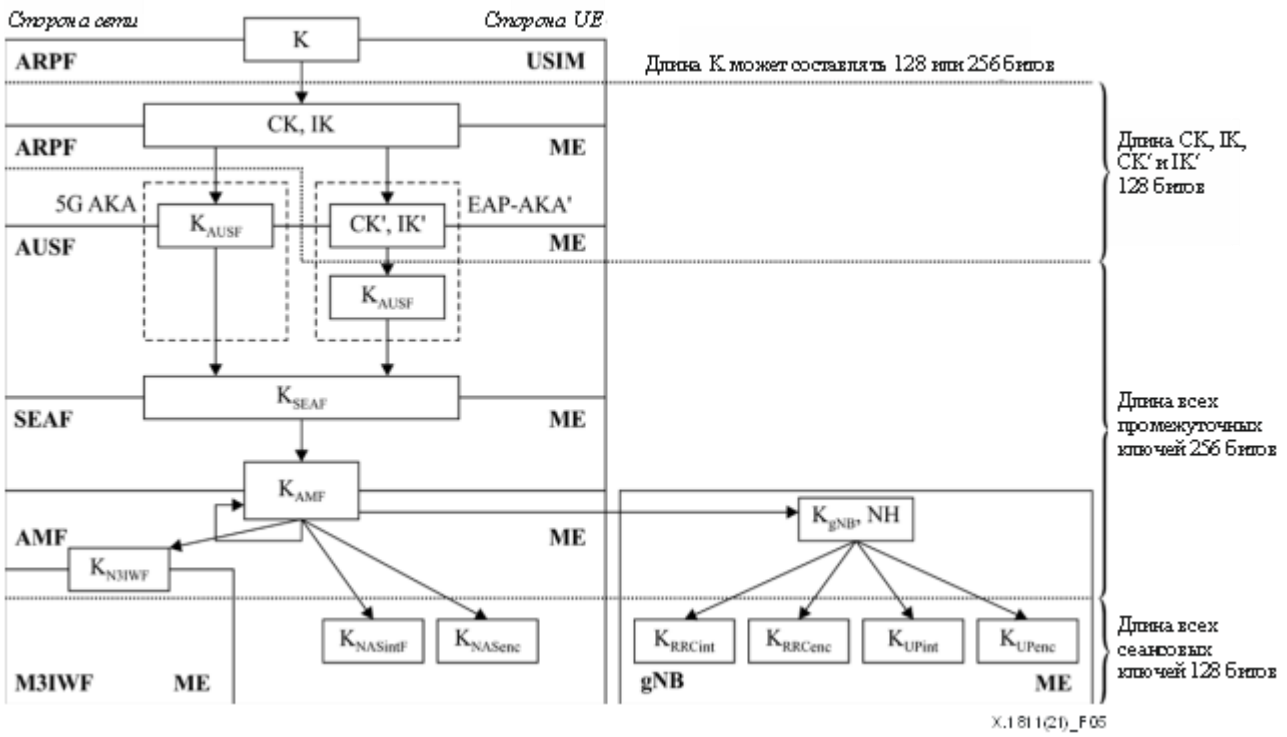


**Рисунок 5 – Иерархия ключей (на основе рисунка 6.2.1-1 из [b-3GPP TS 33.501])**

Длина корневого ключа K может составлять 128 или 256 битов. Стоит отметить, что в унаследованном USIM длина корневого ключа K составляет всего 128 битов, а это означает, что в UDM для соответствующего USIM передаются только 128-битовые корневые ключи.

CK, IK, CK' и IK' – это связанные с процедурой аутентификации ключи длиной 128 битов. Для создания CK и IK используется набор алгоритмов MILENAGE или TUAK, а для создания CK' и IK' – функция выработки общего ключа (GKDF), определенная в [b-3GPP TS 33.220].

Все промежуточные ключи имеют длину 256 битов и создаются с помощью GKDF, за исключением ключа $K_{AUSF}$ в протоколе EAP-AKA'. Для создания $K_{AUSF}$ в протоколе EAP-AKA' используется функция выработки ключа извлечения и расширения на основе HMAC (HKDF), приведенная в [b-IETF RFC 5869].

Ключи ($K_{N3IWF}$, $K_{NASint}$, $K_{NASenc}$, $K_{RRCint}$, $K_{RRCenc}$, $K_{UPint}$, $K_{UPenc}$), используемые для обеспечения защиты связи между UE и сетью, представляют собой 256-битовый выходной код GKDF, усеченный до 128 битов.

#### 7.2.1.4 Безопасность сигнализации NAS, сигнализации AS и пользовательских данных

Для обеспечения конфиденциальности сигнализации NAS, сигнализации AS и пользовательских данных система IMT-2020 должна поддерживать 128-NEA1 (128-битовый алгоритм на основе SNOW 3G) и 128-NEA2 (128-битовый алгоритм на основе AES). Кроме того, в системе IMT-2020 может поддерживаться 128-NEA3 (128-битовый алгоритм на основе ZUC).

Для обеспечения целостности сигнализации NAS, сигнализации AS и пользовательских данных система IMT-2020 должна поддерживать 128-NIA1 (128-битовый алгоритм на основе SNOW 3G) и 128-NIA2 (128-битовый алгоритм на основе AES). Кроме того, в системе IMT-2020 может поддерживаться 128-NIA3 (128-битовый алгоритм на основе ZUC).

#### 7.2.1.5 NDS/IP

Защита интерфейсов между сетью доступа и базовой сетью (то есть интерфейса N2 между gNB и AMF, интерфейса N2 между N3IWF и AMF, интерфейса N3 между gNB и UPF, интерфейса N3 между N3IWF и UPF), интерфейсов между gNB-DU и gNB-CU (интерфейса F1) и между gNB-CU-CP и gNB-CU-UP (интерфейса E1) обеспечивается путем применения протокола NDS/IP ([b-3GPP TS 33.210], [b-3GPP TS 33.310]), который определяет профиль безопасности, используемый в системах 3GPP для IPsec, протокола обмена ключами по интернету версии 2 (IKEv2), TLS и дейтаграмм безопасности транспортного уровня (DTLS) [b-IETF RFC 6083].

Для защиты целостности и конфиденциальности данных, передаваемых по интерфейсу N2, интерфейсу E1 и интерфейсу F1, а также для предотвращения атак повторением рекомендуется использовать инкапсуляцию полезной нагрузки безопасности (ESP) IPsec и аутентификацию на основе сертификатов IKEv2. Кроме того, должен поддерживаться протокол DTLS.

Для обеспечения целостности, конфиденциальности и защиты от атак повторением трафика по интерфейсу N3 рекомендуется использовать IPsec ESP и аутентификацию на основе сертификатов IKEv2.

В качестве алгоритмов шифрования ESP в дополнение к AES-256 должны поддерживаться усовершенствованный стандарт шифрования – сцепление шифрованных блоков (AES-CBC) и усовершенствованный стандарт шифрования – режим счетчика Галуа (AES-GCM) с 16-октетным ICV. В качестве алгоритмов аутентификации ESP должны поддерживаться HMAC-SHA1-96 и усовершенствованный стандарт шифрования – код аутентификации сообщений Галуа (AES-GMAC) с AES-128.

В отношении IKEv2 должны поддерживаться следующие алгоритмы:

– конфиденциальность: ENCR_AES_CBC с длиной ключа 128 битов, AES-GCM с 16-октетным ICV и длиной ключа 128 битов;
– псевдослучайная функция: PRF_HMAC_SHA1, PRF_HMAC_SHA2_256;
– целостность: AUTH_HMAC_SHA256_128;
– группа 14 DH (2048-битовая MODP), группа 19 DH (256-битовая группа случайной ECP).

Для обеспечения высокого уровня безопасности в отношении IKEv2 должны поддерживаться следующие алгоритмы:

– конфиденциальность: AES-GCM с 16-октетным ICV и длиной ключа 256 битов;
– псевдослучайная функция: PRF_HMAC_SHA2_384;
– группа 20 DH (384-битовая группа случайной ECP).

В DTLS 1.2 используются те же наборы шифров, что и в TLS 1.2, поскольку DTLS 1.2, как указано в [b-IETF RFC 6347], основан на TLS 1.2. Необходимо придерживаться разрешенных и обязательных наборов шифров, приведенных в TLS 1.2 [b-IETF RFC 5246]. Кроме того, обязательна поддержка и рекомендуется использование следующих наборов шифров:

– TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, определенный в [b-IETF RFC 5289];

– TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, определенный в [b-IETF RFC 5288].

Для обеспечения высокого уровня безопасности рекомендуется поддержка следующих наборов шифров:

– TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, определенный в [b-IETF RFC 5289];

– TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, определенный в [b-IETF RFC 5289].

В отношении групп DH для ECDHE должны поддерживаться кривые secp256r1 (P-256), как определено в [b-IETF RFC 4492], и secp384r1 (P-384), как определено в [b-IETF RFC 4492]. Для DHE должны поддерживаться группы DH длиной не менее 4096 битов; группы DH длиной менее 2048 битов поддерживаться не должны.

Для использования при квитировании установления связи между IKEv2 и TLS в контексте NDS/IP разрешена аутентификация на основе PSK.

#### 7.2.1.6 Безопасность не-3GPP-доступа

Безопасность не-3GPP-доступа обеспечивается путем установления туннеля IPsec между UE и N3IWF. Чтобы установить одну или несколько ассоциаций безопасности IPsec ESP [b-IETF RFC 4303] для туннелей IPsec, для выполнения взаимной аутентификации между UE и N3IWF на основе ключа $K_{N3IWF}$, используется IKEv2 [b-IETF RFC 7296].

Безопасность связи между N3IWF и AMF (интерфейс N2), а также между N3IWF и UPF (интерфейс N3) обеспечивается с помощью NDS/IP.

### 7.2.2 Безопасность базовой сети

Ожидается, что базовая сеть IMT-2020 будет построена на основе структуры NFV [b-ETSI GS NFV 002], в которой сетевые функции (NF) отделены от специального оборудования в целях быстрого развертывания услуг и повышения эффективности работы. Как показано на рисунке 6, структуру NFV можно разделить на три уровня: NFVI; функции VNF и сетевые службы. Функции VNF работают поверх общего уровня NFVI для предоставления услуг желаемых сетевых служб. Безопасность базовой сети в основном обеспечивается уровнем VNF.

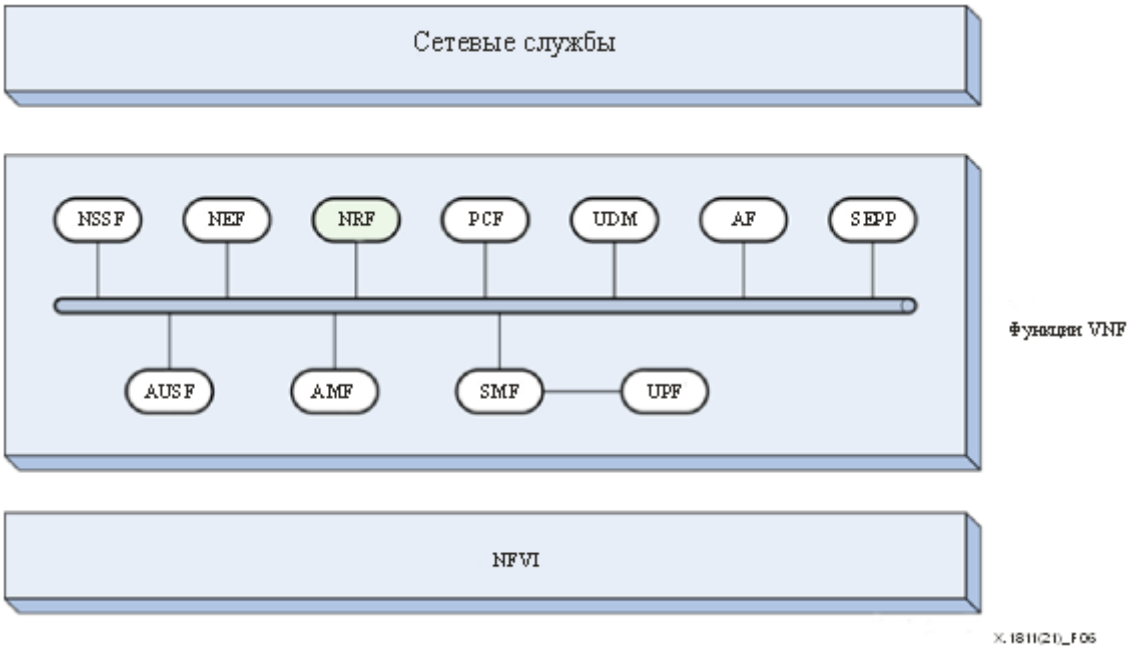


**Рисунок 6 – Структура базовой сети IMT-2020 на основе NFV (на основе рисунка 1 из [b-ETSI GS NFV 002]**

Функции VNF организованы в SBA, где ключевую роль в системе играет функция репозитория NF (NRF). NRF решает, уполномочена ли NF осуществлять обнаружение и регистрацию, и выдает маркер

доступа к NF. Можно рассматривать безопасность уровней VNF в сухопутной подвижной сети общего пользования (PLMN) и между сетями PLMN.

#### 7.2.2.1 Безопасность в сети PLMN

**1) Аутентификация**

NRF и NF должны выполнить взаимную аутентификацию в процессе обнаружения, регистрации и запроса маркера доступа. Это может быть сделано с использованием либо NDS/IP, либо физической защиты. Таким же образом может выполняться аутентификация между NF.

**2) Авторизация**

– **Статическая авторизация**

После взаимной аутентификации NF потребителя услуг и NF поставщика услуг NF поставщика проверяет авторизацию NF потребителя услуг на основе локальной политики, прежде чем предоставить доступ к интерфейсу прикладного программирования (API) услуг.

– **Авторизация на основе OAuth 2.0**

Управление доступом к сетевым службам, предоставляемым NF, может быть реализовано с помощью структуры OAuth 2.0, описанной в [b-IETF RFC 6749]. Маркеры доступа должны быть веб-маркерами JSON (нотации объектов JavaScript), как описано в [b-IETF RFC 7519], защищенными цифровыми подписями или цифровыми подписями MAC на основе веб-подписи JSON (JWS), как описано в [b-IETF RFC 7515]. NRF действует как сервер авторизации OAuth 2.0. Потребитель услуг NF соответствует клиенту OAuth 2.0, а поставщик услуг NF – серверу ресурсов OAuth 2.0. Защита связи между NF и NRF обеспечивается с помощью TLS, поскольку регистрационные данные передаются между ними.

#### 7.2.2.2 Безопасность между PLMN

Безопасность между PLMN обеспечивается периферийными прокси-серверами безопасности (SEPP) обеих сетей через интерфейс N32, как показано на рисунке 7.

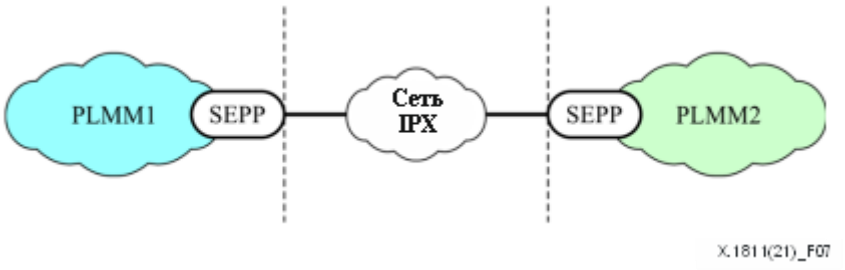


**Рисунок 7 – Обеспечение безопасности между PLMN**

Интерфейс N32 состоит из соединений N32-c и N32-f. Первое соединение отвечает за управление интерфейсом N32, включая взаимную аутентификацию и согласование ключей между двумя SEPP с использованием TLS. Второе отвечает за передачу сообщений, защищенных подписью и шифрованием объектов JavaScript (JOSE), между SEPP.

SEPP используют веб-шифрование JSON (JWE, определенное в [b-IETF RFC 7516]) для защиты сообщений в интерфейсе N32, где применяются согласованные ключи между двумя SEPP в соединении N32-c. Поставщики услуг по обмену трафиком интернета (IPX) применяют JWS, как описано в [b-IETF RFC 7515], для подписания изменений, необходимых для их посреднических услуг.

Все объекты и функции, поддерживающие JWE, должны использовать следующие алгоритмы [b-3GPP-TS 33.210]: должны поддерживаться параметр enc A128GCM (AES-GCM с 128-битовым ключом), параметр enc A256GCM (AES-GCM с 256-битовым ключом), а также alg-параметр dir (прямое использование общего симметричного ключа в качестве ключа шифрования контента (CEK)).

Все объекты и функции, поддерживающие JWS, должны использовать следующие алгоритмы [b-3GPP-TS 33.210]: должен поддерживаться параметр alg ES256 (алгоритм цифровой подписи на

основе эллиптических кривых (ECDSA) с использованием P-256 и защищенного алгоритма хеширования-256 (SHA-256)).

### 7.3 Безопасность плоскости управления

Плоскость управления состоит из набора функций управления (оркестратор NFV, менеджер VNF, менеджер виртуализированной инфраструктуры, контроллер SDN, менеджер RAN). Этот набор отвечает за управление конфигурацией, рабочими характеристиками и ошибками соответствующих объектов через интерфейсы. Во время передачи данных между менеджером и управляемым объектом любые изменения, удаления, вставки или повторения исключаются [b-ETSI GS NFV-SEC 014]. По этой причине в отрасли в отношении этих интерфейсов по умолчанию применяется TLS, как показано на рисунке 8.

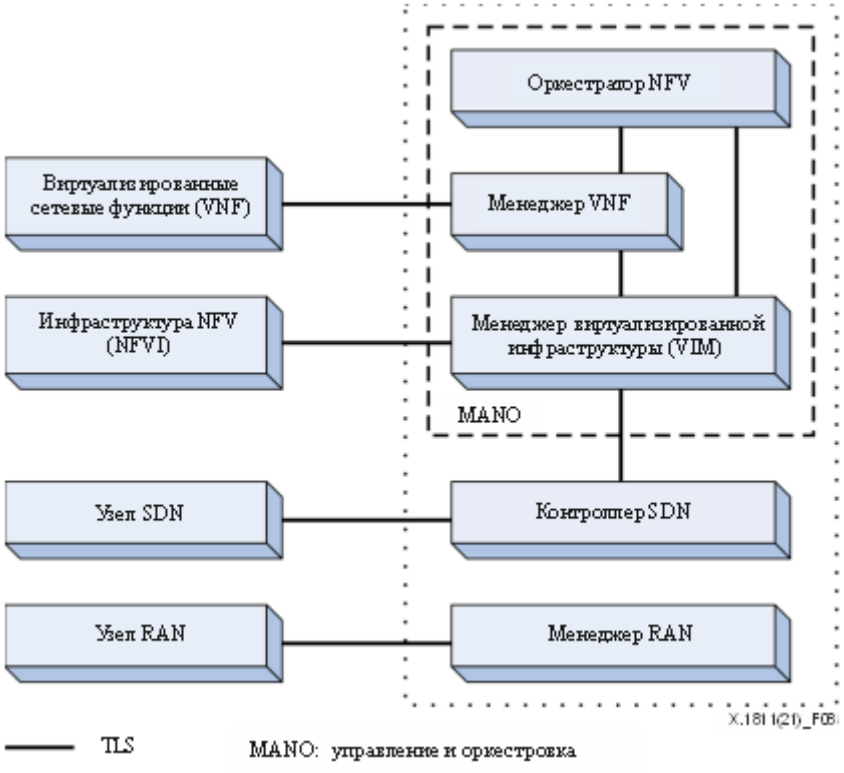


**Рисунок 8 – Безопасность плоскости управления**

### 7.4 Краткое описание криптографических алгоритмов, используемых в системе IMT-2020

Основываясь на введении в архитектуру безопасности системы IMT-2020, содержащемся в пунктах 7.1–7.3, используемые в системе IMT-2020 криптографические алгоритмы можно обобщенно представить в таблице 1.

**Таблица 1 – Криптографические алгоритмы, используемые в системе IMT-2020**

| Тип | Наименование | Функция | Сценарий применения |
|---|---|---|---|
| Симметрич-ные крипто-графические алгоритмы | 128-NEA1 | Шифрование | Защита конфиденциальности между UE и AMF, а также между UE и gNB |
| | 128-NEA2 | | |
| | 128-NEA3 | | |
| | 128-NIA1 | MAC | Защита целостности между UE и AMF, а также между UE и gNB |
| | 128-NIA2 | | |
| | 128-NIA3 | | |
| | AES-128 | Шифрование | IPsec, TLS, DTLS, JWE, ECIES, NFVI |

**Таблица 1 – Криптографические алгоритмы, используемые в системе IMT-2020**

| Тип | Наименование | Функция | Сценарий применения |
|---|---|---|---|
| | AES-256 | Шифрование | IPsec, TLS, DTLS, JWE, NFVI |
| | Blowfish | Шифрование | SDN |
| | 3DES | Шифрование | SDN |
| | SHA-256 | Хеширование | IPsec, TLS, DTLS, JWS, NFVI |
| | SHA-384 | Хеширование | IPsec, TLS, DTLS, JWS, NFVI |
| | HMAC-SHA-256 | Выработка ключей/MAC/ псевдослучайная функция | Иерархия ключей IPsec, TLS, DTLS, JWS, NFVI |
| | HMAC-SHA-384 | Выработка ключей/MAC/ псевдослучайная функция | IPsec, TLS, DTLS, JWS, NFVI |
| Несимме-тричные криптографи-ческие алгоритмы | RSA | Подпись | IPsec, TLS, DTLS, JWS, NFVI |
| | ECDSA | Подпись | IPsec, TLS, DTLS, JWS, NFVI |
| | DH | Соглашение о ключах | IPsec, TLS, DTLS, NFVI |
| | ECDH | Соглашение о ключах | IPsec, TLS, DTLS, NFVI |
| ПРИМЕЧАНИЕ 1. – SHA-1 не указан из-за низкого уровня его безопасности.<br>ПРИМЕЧАНИЕ 2. – Размер ключей используемых в настоящее время несимметричных криптографических алгоритмов не указан, поскольку при наличии мощного квантового компьютера эти алгоритмы могут быть взломаны независимо от размера ключа.<br>ПРИМЕЧАНИЕ 3. – По соображениям безопасности версия TLS не ниже 1.2. | | | |

## 8 Оценка безопасности систем IMT-2020 при квантовых вычислениях

Квантовый компьютер – это устройство, в котором для выполнения вычислений и манипулирования данными используются явления квантовой механики (суперпозиция и запутанность). В основе безопасности популярных в настоящее время криптографических алгоритмов лежат некоторые труднорешаемые математические задачи. Благодаря присущему квантовому компьютеру свойству параллелизма некоторые квантовые алгоритмы позволяют решать сложные математические задачи эффективнее, чем классические алгоритмы. Это создает серьезные и реальные угрозы безопасности для современной криптографии. В Дополнении III показано влияние квантовых вычислений на широко распространенные криптографические алгоритмы. В пункте 8.1 перечислены угрозы, создаваемые квантовыми компьютерами для обычных криптографических алгоритмов. Затем анализируется влияние квантовых компьютеров на системы IMT-2020.

### 8.1 Угрозы обычным криптографическим алгоритмам

#### 8.1.1 Несимметричные криптографические алгоритмы

Алгоритм Шора позволяет решать задачу разложения на множители больших целых чисел и задачу дискретного логарифмирования за полиномиальное время [b-Shor 1999]. Это ставит под угрозу безопасность популярных в настоящее время несимметричных алгоритмов. Отсюда следует, что шифрование с открытым ключом на основе RSA, безопасность которого базируется на задаче разложения на множители больших целых чисел, и протокол обмена ключами DH, безопасность которого базируется на задаче дискретного логарифмирования, перестанут обеспечивать безопасность. Безопасность алгоритма DSA, как и алгоритма DH, опирается на дискретный логарифм. Следовательно, алгоритм DSA подвержен квантовым атакам. ECC, безопасность которого основана на задаче дискретного логарифмирования на эллиптической кривой (ECDLP), получило широкое применение из-за гораздо меньшего размера ключа по сравнению с системой с открытым ключом на основе RSA. Однако его можно взломать, используя вариант алгоритма Шора [b-Roetteler]. Это означает, что при наличии мощных квантовых компьютеров ECC, включая ECDSA и ECDH, небезопасны. В таблице 2 перечислены требуемые для взлома широко используемых несимметричных криптографических алгоритмов ресурсы квантового компьютера.

**Таблица 2 – Ресурсы квантового компьютера, требуемые для взлома широко используемых несимметричных криптографических алгоритмов**

| Алгоритмы | Размер открытого ключа (биты) | Уровень безопасности, сопоставимый с симметричным алгоритмом (биты) | Количество логических кубитов | Количество физических кубитов (см. примечание 1) | Количество элементов Тоффоли (см. примечание 1) | Время, требуемое для взлома алгоритма (см. примечание 2) |
|---|---|---|---|---|---|---|
| RSA [b-Häner] | 1024 | 80 | 2050 | 7,38 × 106 | 5,81 × 1011 | 9,68 часа |
| | 2048 | 112 | 4098 | 1,48 × 107 | 5,2 × 1012 | 3 суток 14 часов |
| | 4096 | 128 | 8194 | 2,95 × 107 | 5,59 × 1013 | 31 сутки 21 час |
| На основе ECC [Roetteler] | 256 | 128 | 2330 | 8,39 × 106 | 1,26 × 1011 | 2,1 часа |
| | 384 | 192 | 3484 | 1,25 × 107 | 4,52 × 1011 | 7,5 часа |
| | 521 | 256 | 4719 | 1,69 × 107 | 1,14 × 1012 | 19 часов |
| ПРИМЕЧАНИЕ 1. – Квантовым компьютерам требуются дополнительные физические квантовые биты для исправления ошибок. Расчетное количество физических кубитов на один логический кубит варьирует от 10 до 10 000. Здесь предполагается, что на один логический кубит приходится 3600 физических кубитов (см. [B-Fowler]).<br>ПРИМЕЧАНИЕ 2. – По нашим предположениям, время срабатывания логического элемента Тоффоли составляет 60 нс (см. [b-Banchi]). | | | | | | |

### 8.1.2 Симметричные криптографические алгоритмы

Алгоритм Гровера обеспечивает квадратичное ускорение поиска в наборе неструктурированных данных по сравнению с классическими алгоритмами [b-Grover]. Это может быть использовано для поиска ключа в пространстве ключей алгоритма с симметричными ключами. Для алгоритма с симметричными ключами длиной $n$ битов ключ можно определить с помощью $O(2^{n/2})$ квантовых операций на квантовом компьютере вместо $O(2^n)$ классических операций на обычном компьютере. Квантовый ресурс, требуемый для поиска ключа симметричного алгоритма, столь велик, что реализация алгоритма Гровера для взлома алгоритма с симметричными ключами на реальном физическом квантовом компьютере вызывает сомнения. Например, для полного поиска ключа AES с использованием алгоритма Гровера необходимо следующее количество логических элементов Тоффоли и Клиффорда: $2^{86}$ для AES-128; $2^{118}$ для AES-192 и $2^{151}$ для AES-256, тогда как количество требуемых логических кубитов колеблется от 3000 до 7000 [b-Grassl].

Алгоритм Гровера сокращает эффективный размер ключа вдвое, то есть вдвое снижает уровень безопасности алгоритма с симметричными ключами. Таким образом, для достижения квантовой безопасности размер ключа алгоритма с симметричными ключами следует удвоить.

### 8.1.3 Алгоритмы хеширования

Алгоритм Гровера и его вариант не ускоряют обнаружение хеш-коллизий по сравнению с классическим алгоритмом [b-Bernstein 2009]. Наилучшим подходом было бы использование параллельной версии метода ρ Полларда на классическом компьютерном кластере [b-ETSI GR QSC 006]. Это означает, что если используемые в настоящее время хеш-алгоритмы являются защищенными, то они будут защищены и от атак на основе квантовых вычислений в квантовую эру. Было установлено, что алгоритм SHA-256, признанный безопасным при использовании классических вычислений, способен противостоять и квантовой атаке на прообраз [b-Amy].

### 8.1.4 Функция выработки ключей

Функции выработки ключей (KDF) предназначены для генерирования ключей, используемых для защиты конфиденциальности и целостности данных, что достигается путем встраивания общего ключа в хеш-функции. В системе IMT-2020 применяются KDF двух типов. Это GKDF, определенный в [b-3GPP TS 33.220], и HKDF, определенный в [b-IETF RFC 5869].

Основой GKDF и HKDF является хеш-функция со встроенным ключом HMAC-SHA-256. Безопасность HMAC зависит от криптостойкости используемой хеш-функции [b-IETF RFC 2104]. В результате

достижения в области квантовых вычислений не оказывают существенного влияния на сами KDF, используемые в системе IMT-2020.

Следует отметить, что энтропия результата KDF зависит от энтропии входного ключа, используемого в KDF. При применении KDF для получения результата с энтропией 256 битов необходим входной ключ с энтропией 256 битов.

### 8.2 Прогноз сроков появления мощного квантового компьютера

Точные сроки появления мощных квантовых компьютеров трудно спрогнозировать, поскольку по этому вопросу нет единого мнения. По оценкам [b-NISTIR 8105], квантовый компьютер стоимостью 1 млрд долл. США сможет взломать 2048-битовый RSA в 2030 году. Европейский институт стандартизации электросвязи (ETCИ) пришел к аналогичному заключению: мощные квантовые компьютеры могут появиться в 2031 году [b-ETSI GR QSC 004]. В результате безопасность систем IMT-2020 может быть поставлена под угрозу, поскольку эти системы должны работать в течение 10–20 лет. С другой стороны, [b-NASEM] заявляет о маловероятности того, что в следующем десятилетии будет построен квантовый компьютер, взламывающий 2048-битовый RSA. Это не означает, что сегодня не требуется изучать и стандартизировать криптографические алгоритмы**,** обеспечивающие квантовую безопасность, поскольку временны́е рамки для перехода к новому алгоритму безопасности достаточно длинны и неопределенны [b-NASEM].

### 8.3 Влияние на системы IMT-2020

Как показано в разделе 7, в развернутых во многих местах сетях IMT-2020 используются протоколы IPsec, TLS и DTLS. Сначала необходимо дать общее представление о них, чтобы оценить угрозы, создаваемые для них квантовыми компьютерами. После этого в соответствии со структурой раздела 7 приводится оценка влияния на безопасность систем IMT-2020.

#### 8.3.1 Влияние на IPsec, TLS и DTLS

Хотя IPsec, TLS и DTLS работают на разных уровнях для защиты передачи сообщений (IPsec – на сетевом уровне, TLS и DTLS – между сетевым уровнем и уровнем приложений), они основаны на схожих принципах. Каждый из них состоит из двух частей: одна касается аутентификации и создания ключей для выработки сеансовых ключей, а другая – защиты конфиденциальности и целостности сообщений с помощью симметричных алгоритмов с сеансовыми ключами.

Существует два метода аутентификации и создания ключей на основе: 1) предварительно распространенного симметричного ключа и 2) открытого ключа (обычно с использованием сертификата).

Для защиты конфиденциальности и целостности текущие наборы алгоритмов шифрования в IPsec, TLS и DTLS могут поддерживать как 128-битовые, так и 256-битовые симметричные алгоритмы.

В результате при рассмотрении случаев 1–4 можно оценить, способны ли IPsec, TLS и DTLS противостоять атакам с применением квантовых вычислений.

**Случай 1.** Аутентификация на основе открытого ключа и 128-битовые или 256-битовые симметричные алгоритмы

В этом случае сеансовые ключи могут быть восстановлены злоумышленниками, поскольку современные несимметричные алгоритмы, указанные в стандартах Целевой группы по инженерным проблемам интернета (IETF), могут быть взломаны квантовыми компьютерами благодаря алгоритму Шора. Таким образом, безопасность передаваемых сообщений не может быть гарантирована независимо от размера ключа симметричных алгоритмов.

**Случай 2.** Аутентификация на основе PSK 128 битов и 128-битовые симметричные алгоритмы

В этом случае при наличии мощного квантового компьютера эффективный размер ключа безопасности из-за алгоритма Гровера составляет 64 бита. Таким образом, эти три протокола не обеспечивают защиту от квантовой атаки.

**Случай 3.** Аутентификация на основе PSK 256 битов и 128-битовые симметричные алгоритмы

В этом случае, хотя для аутентификации и создания ключей используется PSK 256 битов, для защиты сообщений применяются только 128-битовые симметричные алгоритмы. Таким образом, уровень безопасности этих трех протоколов составляет 64 бита.

**Случай 4.** Аутентификация на основе PSK 256 битов и 256-битовые симметричные алгоритмы

В этом случае эффективная степень защиты этих трех протоколов составляет 128 битов. Таким образом, используя этот профиль шифрования, можно отразить квантовые атаки.

При современных профилях шифрования защита от квантовых атак обеспечивается только в случае 4. Однако аутентификация на основе PSK подходит лишь для связи в небольшой группе, поскольку PSK на соответствующих устройствах необходимо настраивать вручную. Для связи в большой группе рекомендуется применять аутентификацию на основе открытого ключа. Для этого в вышеупомянутые протоколы (например, IPsec, TLS и DTLS) рекомендуется включить несимметричные криптографические алгоритмы аутентификации, обеспечивающие квантовую безопасность.

### 8.3.2 Влияние на уровень инфраструктуры

Как показано в пункте 7.1, для защиты интерфейса между приложениями и контроллером SDN, а также интерфейса между контроллером SDN и узлами SDN используется TLS. К интерфейсу между контроллером SDN и узлами SDN может применяться IPsec. На основании анализа, приведенного в пункте 8.3.1, эти два интерфейса подвержены квантовым атакам, то есть злоумышленники могут перехватывать, изменять и внедрять сообщения, передаваемые через эти два интерфейса, если в TLS и IPsec не используются алгоритмы, указанные для случая 4.

Уровень NFVI уязвим для квантовой атаки, поскольку для реализации некоторых функций безопасности он использует классические несимметричные криптографические алгоритмы. Это может привести к серьезным последствиям, таким как незаконный доступ к платформе или установка вредоносного программного обеспечения.

### 8.3.3 Влияние на сеть доступа

#### 8.3.3.1 Неприкосновенность частной жизни абонента

Как описано в пункте 7.2, скрытие идентификатора SUPI осуществляется путем его преобразования в SUCI с помощью схемы ECIES. Для согласования общего ключа между UE и сетью в схеме ECIES используется ECDH. При наличии мощных квантовых компьютеров злоумышленники в результате атаки могут восстановить общий ключ с помощью алгоритма Шора. Следовательно, они могут раскрыть SUPI, расшифровав SUCI с использованием общего ключа.

#### 8.3.3.2 Аутентификация

Протоколы AKA и EAP-AKA' 5G выполняют взаимную аутентификацию между UE и сетью на основе долговременного ключа K, размер которого может составлять 128 или 256 битов. Что касается 256-битового ключа K, то до сих пор отсутствовали какие-либо атаки с применением классического компьютера на хеш-функции (то есть набор алгоритмов TUAK), составляющие основу для получения различных параметров, используемых в протоколе аутентификации. Таким образом, оба протокола аутентификации защищены от квантовых атак, поскольку более эффективного алгоритма для взлома хеш-функций с помощью квантовых компьютеров, чем 256-битовый ключ K, не существует. Что же касается 128-битового ключа K, эффективная степень защиты которого в квантовую эру составит 64 бита, то злоумышленники могут восстановить ключ K из захваченных сообщений, относящихся к обоим протоколам аутентификации, например AV, путем выполнения $2^{64}$ квантовых операций с использованием алгоритма Гровера.

#### 8.3.3.3 Иерархия ключей

Иерархия ключей используется для получения 128-битовых ключей из долговременного (корневого) ключа K, как показано на рисунке 5, в целях обеспечения защиты связи между UE и сетью. В настоящее время широко применяется ключ K длиной 128 битов, тогда как ключ K длиной 256 битов используется довольно редко. Что касается 128-битового ключа K, эффективная степень защиты которого в квантовую эру составит 64 бита, уровень безопасности его производных ключей составляет 64 бита. В результате предпринимающие атаку злоумышленники смогут восстановить ключи по перехваченным сообщениям, зашифрованным с помощью 128-битовых ключей.

#### 8.3.3.4 Сигнализация NAS, сигнализация AS и пользовательские данные

Защита конфиденциальности сигнализации NAS, сигнализации AS и пользовательских данных обеспечивается с помощью симметричных алгоритмов с ключами длиной 128 битов. Таким образом, эти сообщения могут быть расшифрованы злоумышленниками с помощью квантовых компьютеров.

Защита целостности сигнализации NAS, сигнализации AS и пользовательских данных обеспечивается с помощью алгоритмов MAC с 128-битовым ключом. Выходные данные алгоритмов MAC усекаются в тег длиной 32 бита, который используется в качестве тега MAC. Если длина тега MAC составляет 32 бита, то злоумышленник может подделать сообщение после 231 попытки. Вопрос о том, окажется ли безопасность системы IMT-2020 под угрозой, если 32-битовый тег MAC получен путем усечения 64-битового или 128-битового исходного тега, требует дальнейшего изучения.

#### 8.3.3.5 NDS/IP

Для защиты интерфейсов N2, N3, E1 и F1 применяются TLS, DTLS и IPsec, как описано в пункте 7.2.1. Они подвержены такому же влиянию, как и транспортный уровень, то есть злоумышленники могут перехватывать, изменять и внедрять сообщения, передаваемые по этим интерфейсам, если не используются наборы шифров, указанные для случая 4 в пункте 8.3.1.

#### 8.3.3.6 Безопасность не-3GPP-доступа

Защита не-3GPP-доступа обеспечивается с помощью IPsec. По причинам, изложенным в пункте 8.3.1, безопасный не-3GPP-доступ не может быть гарантирован, если не используются наборы шифров, указанных для случая 4 в пункте 8.3.1.

### 8.3.4 Влияние на базовую сеть

#### 8.3.4.1 Безопасность в сети PLMN

**1) Аутентификация**

Аутентификация между сетевыми функциями NF не будет затронута, если ее осуществление основано на физической защите. Если же аутентификация обеспечивается с использованием NDS/IP, то она может быть подвержена тем же угрозам, какие указаны в пункте 8.3.3.

**2) Авторизация**

Статическая авторизация не подвержена воздействию, поскольку для нее не применяются какие-либо криптографические алгоритмы.

В случае авторизации на основе OAuth 2.0 существует два сценария обеспечения целостности маркера доступа. Злоумышленник может подделать маркер доступа, если его целостность защищена с помощью подписи. Если же для защиты целостности маркера доступа применяется MAC с ключом длиной 256 битов, его подделать нельзя. Регистрационные данные, используемые при авторизации, могут быть раскрыты при передаче по протоколу TLS между NF, если не применяются алгоритмы, указанные для случая 4 в пункте 8.3.1.

#### 8.3.4.2 Безопасность между PLMN

Злоумышленники могут перехватывать, изменять и внедрять сообщения, передаваемые между PLMN по интерфейсу N32. Причина в том, что для создания сеансовых ключей соединение N32-c полагается на аутентификацию на основе сертификатов в TLS, и злоумышленники могут получить эти ключи с помощью квантовых компьютеров.

### 8.3.5 Влияние на плоскость управления

Во время передачи данных между менеджером и управляемыми объектами возможна любая их модификация, удаление, вставка или повторение, поскольку в плоскости управления применяется TLS с аутентификацией на основе сертификатов. Это представляет серьезную угрозу для систем IMT-2020, потому что злоумышленник может получить доступ к системе управления сетью IMT-2020.

## 9 Криптографические алгоритмы, обеспечивающие квантовую безопасность

Квантовые компьютеры создают совершенно новую парадигму вычислений. Она повлияет на безопасность как алгоритмов с симметричными ключами (например, блочных шифров), так и алгоритмов с открытым ключом (таких как RSA), хотя степень влияния для каждого из них будет разной.

В [b-Moses] показано, что для любого алгоритма с симметричными ключами квантовые вычисления вдвое уменьшают количество битов, определяющих стойкость ключа, и что квантовые компьютеры могут выполнять алгоритмы (например, алгоритмы [b-Grover]) и находить ключ симметричного шифра с $N$-битовым ключом за $2^{N/2}$ операций. Таким образом, если квантовые вычисления станут реальностью, то алгоритмы с симметричными ключами можно будет защитить, просто удвоив размер ключа. Безусловно, это повлияет на быстродействие алгоритма с симметричными ключами.

Что же касается алгоритмов с несимметричными ключами, таких как RSA, DSA, ECC и DH, то влияние квантовых вычислений, как предполагается, будет довольно серьезным. Квантовые компьютеры могут выполнять алгоритмы (например, алгоритмы [b-Shor 1997]), которые взламывают все популярные системы с открытым ключом за незначительное время. Например, квантовый алгоритм, называемый алгоритмом Шора, позволяет восстановить ключ RSA за полиномиальное время [b-Moses].

Криптографические алгоритмы**,** обеспечивающие квантовую безопасность, следует выбирать по критериям оценки (см., например, критерии оценки NIST в Дополнении IV).

### 9.1 Алгоритмы с симметричным ключом, обеспечивающие квантовую безопасность

Широко распространено мнение, что базовые симметричные криптосистемы, такие как блочные шифры или хеш-функции, представляют собой алгоритмы, обеспечивающие квантовую безопасность [b-CSA], как показано в Дополнении III. В [b-ITU-T X.1197] содержится список примеров алгоритмов и длин ключей, обеспечивающих квантовую безопасность. В частности, при появлении криптографически значимых квантовых компьютеров потребуется вдвое увеличить размер симметричного ключа по сравнению с современными 128-битовыми ключами, используемыми в системах IMT-2020. В [b-CSA] указывается, что рекомендуемый в настоящее время размер ключа 256 битов считается безопасным даже против алгоритма Гровера.

### 9.2 Алгоритмы с несимметричным ключом, обеспечивающие квантовую безопасность

Хотя квантовые компьютеры могут выполнять алгоритмы, взламывающие современные системы с открытым ключом (например, RSA и ECC) за незначительное время, как показано в Дополнении III, существует множество важных классов криптографических систем помимо RSA и ECC, которые защищают от атак с применением квантовых компьютеров и описаны в пунктах 9.2.1–9.2.5. Список современных стандартов несимметричных алгоритмов, обеспечивающих квантовую безопасность, приведен в [b-ITU-T X.1197].

ПРИМЕЧАНИЕ. – Квантовое распределение ключей (QKD) – это метод реализации соглашения о ключах, надежность которого в отношении квантовых вычислений доказана.

#### 9.2.1 Алгоритмы на основе решетки

Алгоритмы на основе решетки базируются на некоторых хорошо известных сложных задачах на решетке для построения криптографических примитивов, обеспечивающих квантовую безопасность. Одна из них – задача поиска кратчайшего вектора (SVP), то есть задача найти кратчайший ненулевой вектор в заданной решетке, которая, как было доказано, представляет собой трудоемкую недетерминированную полиномиальную задачу (задачу класса NP) с рандомизированными редукциями [b-Ajtai].

В [b-CSA] показано, что алгоритмы на основе решетки могут обеспечивать цифровую подпись, шифрование с открытым или секретным ключом и согласование ключей. Некоторые алгоритмы на основе решетки перечислены в разделе II.1.

### 9.2.2 Алгоритмы на основе хеширования

Алгоритмы на основе хеширования базируются на безопасности базовой криптографической хеш-функции.

В [b-CSA] показано, что алгоритмы на основе хеширования используются для цифровых подписей, построенных с применением хеш-функций. Некоторые алгоритмы на основе хеширования перечислены в разделе II.2.

### 9.2.3 Алгоритмы на основе кодирования

Алгоритмы на основе кодирования используют некоторые коды с исправлением ошибок, где схемы кодирования с трудом поддаются эффективному декодированию даже с применением квантового компьютера. Например, криптосистема Мак-Элиса [b-McEliece] основана на задаче декодирования общего линейного кода класса NP.

В [b-CSA] показано, что алгоритмы на основе кодирования могут обеспечивать цифровую подпись, шифрование с открытым или секретным ключом и согласование ключей. Некоторые алгоритмы на основе кодирования перечислены в разделе II.3.

### 9.2.4 Многомерные алгоритмы

Многомерные алгоритмы основаны на трудности решения систем нелинейных многомерных полиномиальных уравнений над конечными полями. Эта задача считается задачей класса NP [b-Garey].

В [b-CSA] показано, что многомерные алгоритмы могут обеспечивать цифровую подпись и шифрование с открытым или секретным ключом. Некоторые практические схемы подписи, основанные на многомерных алгоритмах, приведены в разделе II.4.

### 9.2.5 Алгоритмы на основе суперсингулярной изогении

Алгоритмы на основе суперсингулярной изогении опираются на трудность восстановления неизвестной изогении между парой суперсингулярных эллиптических кривых, о которых известно, что они являются изогенными.

Эти алгоритмы обеспечивают совершенную прямую секретность и служат простой заменой методов DH и ECDH, устойчивой к квантовым вычислениям. Типичным примером является алгоритм Диффи – Хеллмана с использованием суперсингулярных изогений (SIDH) [b-Jao].

## 10 Руководящие указания по использованию в системах IMT-2020 криптографических алгоритмов, обеспечивающих квантовую безопасность

Сначала приводятся общие соображения о том, как справиться со значительным увеличением размера сообщений при введении в системы IMT-2020 несимметричных алгоритмов, обеспечивающих квантовую безопасность. Затем рассматривается использование криптографических алгоритмов, обеспечивающих квантовую безопасность, в IPsec, TLS и DTLS, поскольку последние применяются во многих уже развернутых системах IMT-2020. И наконец, приводятся руководящие указания по применению криптографических алгоритмов, обеспечивающих квантовую безопасность, в сети доступа и базовой сети IMT-2020.

### 10.1 Размер сообщений

Размер сообщений, содержащих открытый ключ, зашифрованный текст или подпись, значительно увеличится, поскольку в несимметричных алгоритмах, обеспечивающих квантовую безопасность, открытые ключи, зашифрованный текст и подпись обычно имеют гораздо больший размер по сравнению с классическими несимметричными алгоритмами. Например, как показано в разделе II.5, размер открытого ключа несимметричных алгоритмов, обеспечивающих квантовую безопасность, варьирует от 726 байтов до примерно 1 МБ, в то время как открытый ключ классических несимметричных алгоритмов обычно бывает размером от 32 до 256 байтов. Национальный институт

стандартов и технологий (NIST) планирует стандартизировать несколько несимметричных алгоритмов, обеспечивающих квантовую безопасность. Понятно, что для использования в системах IMT-2020 необходимо выбирать несимметричные алгоритмы, обеспечивающие квантовую безопасность, с меньшим размером открытого ключа, зашифрованного текста или подписи. Более того, стандарты систем IMT-2020 должны определять подходящий размер сообщений для размещения открытого ключа, зашифрованного текста или подписи при внедрении несимметричных алгоритмов, обеспечивающих квантовую безопасность.

### 10.2 IPsec, TLS и DTLS

В случае применения для аутентификации и согласования ключей PSK рекомендуется использовать PSK размером 256 битов, а для защиты конфиденциальности и целостности сообщений, передаваемых по сети, рекомендуется использовать симметричные алгоритмы, обеспечивающие квантовую безопасность, с длиной ключа 256 битов. Если используются схемы аутентификации на основе сертификатов, то в протоколы аутентификации для обеспечения квантовой безопасности аутентификации и согласования сеансового ключа рекомендуется встраивать несимметричные алгоритмы, обеспечивающие квантовую безопасность, а для защиты конфиденциальности и целостности сообщений – применять симметричные алгоритмы, обеспечивающие квантовую безопасность, с ключом длиной 256 битов. Это сделает SDN, NDS/IP и плоскость управления неуязвимыми для квантовых атак.

IETF не приступала к работе над способами добавления алгоритмов, обеспечивающих квантовую безопасность, в наборы шифров IPsec, TLS и DTLS, поскольку NIST еще не выбрал окончательных кандидатов на роль несимметричных алгоритмов, обеспечивающих квантовую безопасность. Ожидается, что проекты стандартов NIST появятся в 2022–2024 годах [b-Moody]. Когда IETF определит устойчивые к квантовым атакам наборы шифров для IPsec, TLS и DTLS, для систем IMT-2020 рекомендуется выбрать набор шифров с наименьшим размером ключа и высокой скоростью шифрования с учетом ограниченной пропускной способности беспроводной сети и ограниченных вычислительных возможностей устройств.

### 10.3 Уровень инфраструктуры

Рекомендуется, чтобы в отношении использования IPsec и TLS в SDN применялись предложения, приведенные в пункте 10.2.

Рекомендуется заменить классические криптографические алгоритмы, используемые на уровне NFVI, криптографическими алгоритмами, обеспечивающими квантовую безопасность, в том числе симметричного и несимметричного типов.

### 10.4 Сеть доступа IMT-2020

#### 10.4.1 Неприкосновенность частной жизни абонента

В схеме ECIES для выработки общего ключа рекомендуется применять DH-подобные несимметричные алгоритмы, обеспечивающие квантовую безопасность, такие как инкапсуляция ключей с использованием суперсингулярных изогений (SIKE) и NewHope, которые являются кандидатами второго раунда в процедуре стандартизации постквантовой криптографии (PQC) NIST (см. Дополнение II). Идентификатор SUCI рекомендуется скрывать с помощью симметричного алгоритма, обеспечивающего квантовую безопасность, с 256-битовым общим ключом.

#### 10.4.2 Аутентификация

Поскольку набор алгоритмов MILENAGE поддерживает только входные данные с 128-битовым ключом, а набор алгоритмов TUAK может поддерживать 256-битовый ключ, в процедуре аутентификации для генерации AV и ответа аутентификации вместо MILENAGE рекомендуется использовать набор алгоритмов TUAK.

#### 10.4.3 Иерархия ключей

Чтобы генерировать сеансовый ключ $K_{SEAF}$ с 256-битовой энтропией, в иерархию ключей необходимо внести следующие изменения: 1) рекомендуется, чтобы размер корневого ключа K составлял 256 битов; 2) рекомендуется больше не усекать 256-битовый результат GKDF.

На практике длина корневого ключа K обычно составляет 128 битов из-за использования в системах IMT-2020 унаследованных USIM-карт с такой конфигурацией; новые USIM-карты, используемые многими операторами для ранних систем IMT-2020, по-прежнему будут хранить только 128-битовый корневой ключ. Вследствие этого энтропия сеансового ключа $K_{SEAF}$, полученного из ключа K, составляет всего 128 битов, что не обеспечивает квантовую безопасность.

Чтобы повысить безопасность текущего сеансового ключа $K_{SEAF}$, когда USIM-карта оснащена 128-битовым корневым ключом, выработка такого ключа $K_{SEAF}$ должна быть основана не только на первом сеансовом ключе $K_{SEAF}'$, определяемом долговременным ключом K, но и хотя бы на одном из дополнительных ключей. Дополнительными ключами могут служить начальный сеансовый ключ $K_{SEAF\_INITIAL}$, созданный при первом подсоединении UE к сети, и/или сеансовый ключ $K_{SEAF\_PRV}$, использовавшийся в предыдущем сеансе. И первый сеансовый ключ, и дополнительные ключи являются симметричными ключами, что означает, что UE и сеть используют их совместно. Таким образом, энтропия текущего сеансового ключа $K_{SAEF}$ составит не менее 256 битов, поскольку энтропия первого сеансового ключа $K_{SEAF}'$ составляет 128 битов, а энтропия дополнительных ключей ($K_{SEAF\_INITIAL}$ и/или $K_{SEAF\_PRV}$) – минимум 128 битов.

В качестве примера передовой практики новые SIM-карты необязательно можно использовать для обеспечения 256-битовой энтропии сеансового ключа $K_{SEAF}$. Это могут быть SIM-, USIM- или eSIM-карты или SIM-карты других нестандартных форм-факторов и типов с соответствующими адаптациями:

a) для хранения 256-битового корневого ключа, который служит для той же цели, что и корневой ключ K в старых (U)SIM-картах;

b) для поддержки аппаратного ускорения для необходимой KDF и базового цикла симметричной криптографии (например, AES) в новых SIM-картах. Это особенно актуально для IoT и в тех странах, где значительную долю в общем количестве используемых сотовых устройств составляют телефоны с расширенными функциональными возможностями, которые можно сделать совместимыми с сетями IMT-2020, обеспечивающими если не быстродействие, то квантовую безопасность за счет повторного использования частот и трансляции протоколов.

### 10.4.4 Безопасность сигнализации NAS, сигнализации AS и пользовательских данных

Как показано в разделе 7, основой для защиты конфиденциальности и целостности сигнализации NAS, сигнализации AS и пользовательских данных в сети доступа IMT-2020 служат 128-битовые алгоритмы с симметричными ключами, такие как AES-128, SNOW 3G и ZUC-128.

Чтобы противостоять квантовым атакам, в системах IMT-2020 рекомендуется использовать алгоритмы с 256-битовыми симметричными ключами. Увеличенный размер MAC повышает гарантии защиты от атак с угадыванием MAC сообщения. В [b-NIST SP 800-38B] для защиты от атак с угадыванием рекомендуется использовать MAC длиной не менее 64 битов. Длина MAC в сети доступа IMT-2020 составляет всего 32 бита. Увеличение размера MAC с 32 до 64 битов окажет существенное влияние на сеть и протокол IMT-2020. Вопрос о том, сможет ли сеть доступа IMT-2020 сохранить защищенность от атак с угадыванием при применении 256-битовых симметричных алгоритмов, обеспечивающих квантовую безопасность, для выработки 32-битового MAC, требует дальнейшего изучения.

### 10.4.5 Безопасность не-3GPP-доступа

Для получения информации о стратегии противодействия квантовым атакам для не-3GPP-доступа см. пункт 10.2, поскольку безопасность не-3GPP-доступа зависит от IPsec.

## 10.5 Базовая сеть IMT-2020

### 10.5.1 Безопасность в сети PLMN

#### 1) Аутентификация

Чтобы противостоять квантовым атакам, при аутентификации на основе NDS/IP рекомендуется применять ту же стратегию, какая описана в пункте 10.2.

#### 2) Авторизация

В OAuth 2.0 для обеспечения целостности маркера доступа рекомендуется применять хеш-функции с ключом, обеспечивающим квантовую безопасность, такие как HMAC-SHA-256, и алгоритмы подписи,

обеспечивающие квантовую безопасность. Для получения информации о стратегии перехода на наборы шифров, обеспечивающих квантовую безопасность, в TLS см. пункт 10.2.

Для JWS рекомендуется использовать алгоритмы подписи, обеспечивающие квантовую безопасность.

### 10.5.2 Безопасность между PLMN

Чтобы предотвратить получение злоумышленником, предпринимающим квантовую атаку, сеансовых ключей, в отношении N32-c рекомендуется применять метод, приведенный в пункте 10.2. В интерфейсе N32 для обеспечения конфиденциальности и целостности сообщения между PLMN рекомендуется использовать AES-GCM с 256-битовым ключом.

Для JWS вместо ECDSA рекомендуется использовать алгоритмы подписи, обеспечивающие квантовую безопасность.

# Дополнение I

# Обзор системы 5G

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В данном Дополнении содержится общее описание системы IMT-2020.

## I.1 Общая архитектура

Система IMT-2020 предназначена для предоставления широкого спектра услуг с различными требованиями к их характеристикам. В соответствии со спецификациями 3GPP услуги, предоставляемые в сетях IMT-2020, можно разделить на три категории: 1) услуги eMBB – поддерживают более высокие скорости передачи данных и большую мобильность пользователей, чем 4G/LTE; 2) услуги mIoT – обеспечивают массовую связь машинного типа; 3) услуги URLLC – поддерживают критически важные услуги, для которых требуется повышенная надежность и короткая задержка. Система IMT-2020 должна стать гибкой платформой, позволяющей создавать новые бизнес-модели и интегрировать вертикальные отрасли, такие как автомобилестроение, промышленное производство, энергетика, электронное здравоохранение и развлечения. Кроме того, должны упроститься развертывание и обслуживание системы IMT-2020 по сравнению с подвижными сетями предыдущих поколений. Для удовлетворения этих сложных требований в системе IMT-2020 представлен ряд инновационных технологий, таких как нарезка сети, NFV, SDN, SBA и разделение на центральный и распределенные блоки (CU/DU).

Общую архитектуру системы IMT-2020, показанную на рисунке I.1, можно разделить на следующие функциональные уровни: уровень инфраструктуры; сетевой уровень; уровень обслуживания и плоскость управления.

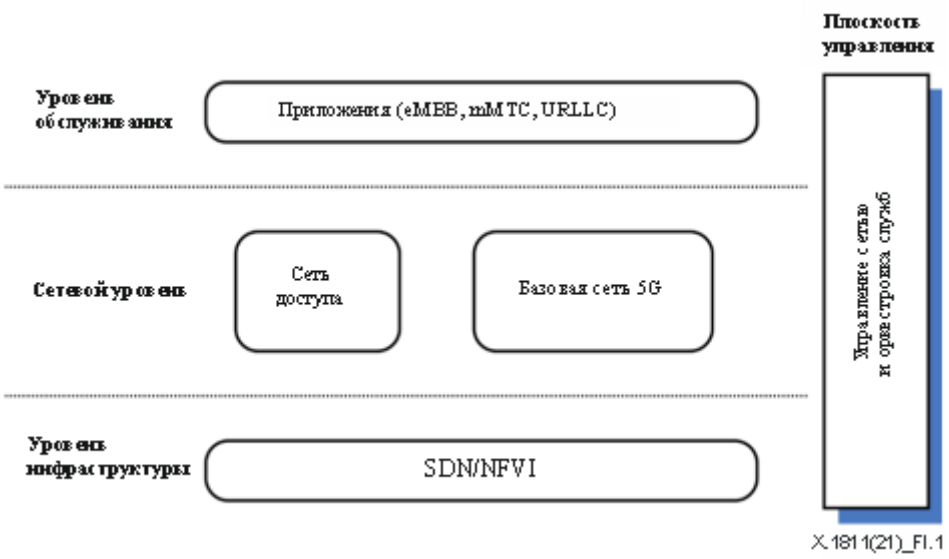


**Рисунок I.1 – Общая архитектура системы IMT-2020**

– Уровень инфраструктуры, включающий SDN и NFVI. SDN используется для транспортировки пакетов к месту назначения. К традиционным технологиям транспортировки (например, многопротокольная коммутация по меткам (MPLS)) в системе IMT-2020 добавлена технология SDN для повышения скорости транспортировки и упрощения адаптации к требованиям к услугам. NFVI служит общей основой для выполнения VNF.

– Сетевой уровень, состоящий из сети доступа и базовой сети. Первая позволяет UE получить доступ к сети IMT-2020 в любом месте. Вторая разработана с учетом SBA для обеспечения расширяемости и простоты. Она состоит из ряда NF для поддержки передачи данных и развертывания служб, таких как AUSF, AMF и SMF.

– Уровень обслуживания, состоящий из приложений, работающих поверх системы IMT-2020, которые могут быть приложениями eMBB, приложениями массовой связи машинного типа (mMTC) и приложениями URLLC.

– Плоскость управления, отвечающая за управление сетью и оркестровку служб.

## I.2 SDN

Основной принцип SDN заключается в том, что плоскость данных отделена от плоскости управления (CP), что позволяет обеспечить возможность динамического программирования узлов сети в процессе пересылки данных. Контроллер SDN принимает решения по управлению сетью и передает полученные правила пересылки узлам сети. Такой механизм пересылки упрощает реализацию узлов сети и приводит к улучшению характеристик плоскости данных. Архитектура SDN представлена на рисунке I.2.

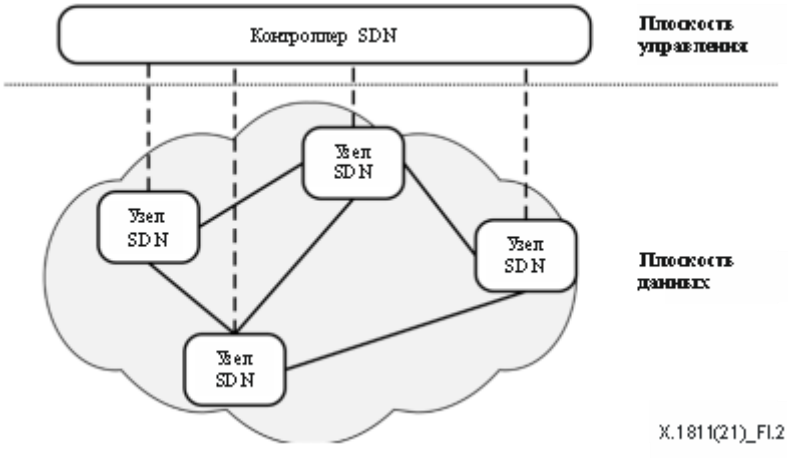


**Рисунок I.2 – Архитектура SDN**

## I.3 Сеть доступа

UE может получить доступ к базовой сети IMT-2020 в режиме либо недоверенного не-3GPP-доступа, либо 3GPP-доступа, как показано на рисунке I.3. Сеть доступа предоставляет услуги, связанные с передачей данных по радиоинтерфейсу.

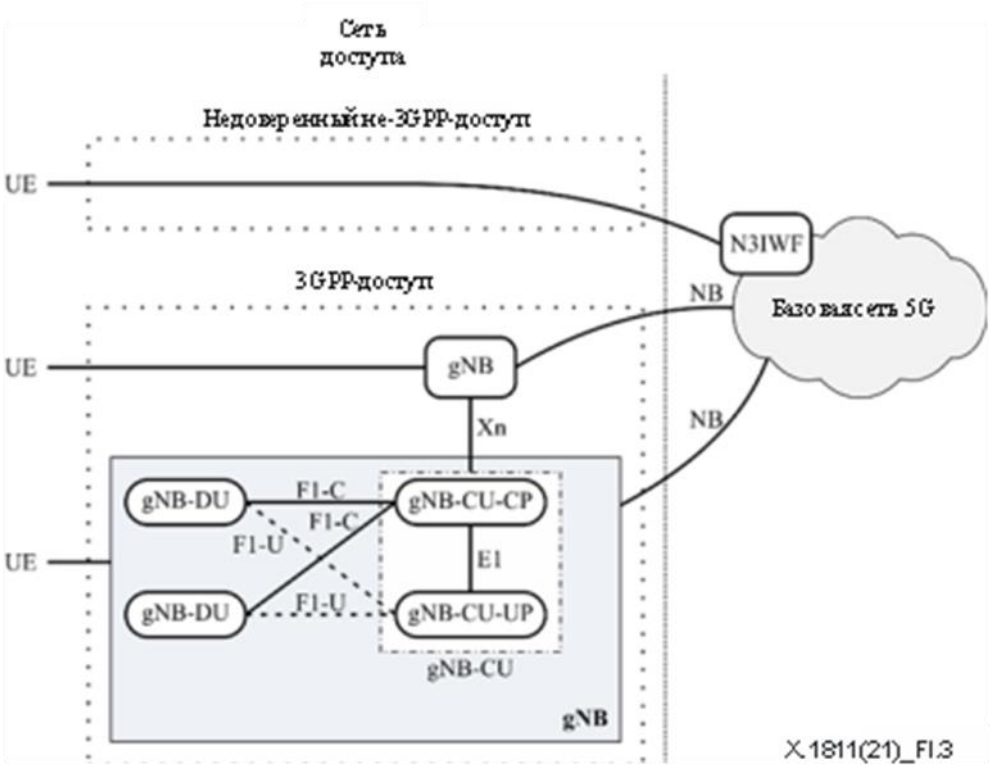


**Рисунок I.3 – Сеть доступа**

– **Недоверенный не-3GPP-доступ**

Недоверенный не-3GPP-доступ, например доступ через беспроводную локальную сеть (WLAN), означает, что технология доступа не указана в стандарте 3GPP и не пользуется доверием базовой сети IMT-2020. В этом контексте UE подключается к базовой сети IMT-2020 через N3IWF.

– **3GPP-доступ**

3GPP-доступ – это технология доступа, описанная 3GPP, то есть технология сетей радиодоступа последующих поколений (NG-RAN) в контексте IMT-2020. UE может получить доступ к базовой сети IMT-2020 с использованием интерфейса NG через плоский gNB без разделения CU/DU. Интерфейс NG представляет собой логический интерфейс, поддерживающий обмен информацией плоскости управления (CP) и информацией плоскости пользователя (UP) между gNB и базовой сетью IMT-2020. Для более гибкого развертывания сети и снижения затрат gNB можно разделить на gNB-DU и gNB-CU. gNB-CU – это логический узел, который выполняет протоколы более высокого уровня, включая протокол адаптации служебных данных (SDAP), протокол управления радиоресурсами (RRC) и протокол сходимости пакетных данных (PDCP). gNB-DU – это логический узел, который выполняет функции нижнего уровня, включая управление радиоканалом (RLC), управление доступом к среде передачи (MAC) и функции физического уровня.

gNB-CU, заимствованный из концепции SDN, можно далее разделить на gNB-CU-CP и gNB-CU-UP. Это приведет к функциональной декомпозиции процесса радиодоступа между пользователем и объектами CP. Такое разделение CP и UP обеспечивает гибкость в работе сложных сетей и управлении ими, позволяя поддерживать различные топологии сети, ресурсы и требования к новым услугам.

Модули gNB-CU и gNB-DU подключаются через логический интерфейс F1, который можно подразделить на интерфейсы F1-C для подключения gNB-CU-CP и F1-U для подключения gNB-CU-UP. gNB-CU-CP поддерживает связь с gNB-CU-UP через интерфейс E1.

## I.4 Базовая сеть

Базовая сеть IMT-2020 определяется как SBA, как показано на рисунке I.4. В SBA определен ряд NF для различных целей. Каждая NF предоставляет набор услуг, называемых услугами NF, которые

потребляются другими авторизованными NF. Для обнаружения и связи друг с другом NF обращаются к NRF.

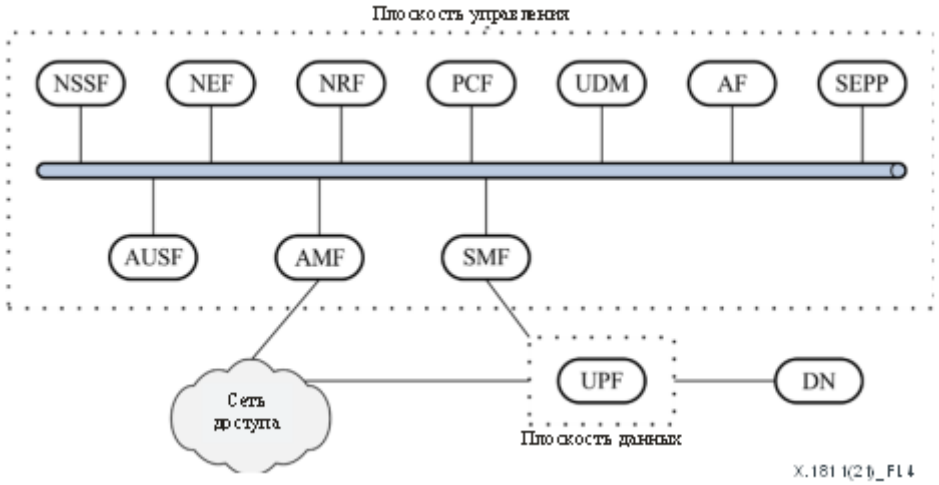


**Рисунок I.4 – Базовая сеть IMT-2020**

Базовую сеть IMT-2020 можно разделить на CP и UP.

– **Плоскость управления**

  Эта плоскость предоставляет услуги управления сетью, включая обеспечение доступа, управление мобильностью, политикой, представления, полицейский перехват и управление начислением платы. В CP определены следующие NF.

– **Функция выбора сетевого сегмента** (NSSF), используемая для выбора набора экземпляров сетевого сегмента, обслуживающего UE.

– **Функция представления сети** (NEF), поддерживающая представление возможностей и событий. Посредством NEF NF предоставляют возможности и события другим NF. Возможности и события, представляемые NF, могут безопасно предоставляться, например, третьим сторонам, функциям приложений и периферийным вычислительным устройствам.

– **Функция репозитория NF** (NRF), обеспечивающая функции регистрации и обнаружения, чтобы NF могли обнаруживать друг друга и устанавливать связь друг с другом через API.

– **Функция управления политикой** (PCF), поддерживающая единую структуру политики для управления поведением сети.

– **Единое управление данными** (UDM), обеспечивающее хранение данных и профилей абонентов. UDM также используется для выработки AV для AKA 3GPP.

– **Функция приложения** (AF), взаимодействующая с базовой сетью 3GPP в целях предоставления услуг. AF также предоставляет информацию о потоке пакетов в PCF.

– **Периферийный прокси-сервер безопасности** (SEPP), представляющий собой непрозрачный прокси-сервер, используемый для защиты сообщений, передаваемых по интерфейсам CP между PLMN, и скрытия топологии сети внутри PLMN.

– **Функция сервера аутентификации** (AUSF), обрабатывающая запросы аутентификации как для 3GPP-, так и для не-3GPP-доступа.

– **Функция управления доступом и мобильностью** (AMF), обеспечивающая управление аутентификацией, авторизацией и мобильностью UE.

– **Функция управления сеансом** (SMF), используемая для управления сеансом, например в целях установления, изменения и прекращения сеанса. SMF также распределяет IP-адреса среди UE.

– **Плоскость пользователя**

**Функция плоскости пользователя** (UPF) – это уникальная функция, определенная для UP. UPF поддерживает различные операции и функции, связанные с пакетами UP, такие как маршрутизация и пересылка пакетов, обработка трафика, проверка пакетов и дублирование пакетов.

Базовая сеть IMT-2020 значительно отличается от базовой сети подвижных сетей предыдущего поколения следующими особенностями.

– **SBA**, службы которой работают с большей степенью детализации, чем в традиционных сетях, и слабо связаны друг с другом. Это позволяет в короткие сроки выводить на рынок новые услуги и обеспечивает большую гибкость при обновлениях системы.

– **Разделение плоскости управления и плоскости пользователя**, позволяющее развернуть UPF в месте, приближенном к UE, с тем чтобы могли быть выполнены строгие требования к задержке со стороны услуг URLLC. Разделение плоскости управления и плоскости пользователя также позволяет независимо масштабировать ресурсы каждой плоскости.

– **Разделение AMF и SMF**, позволяющее осуществлять централизованное управление доступом и мобильностью. SMF, напротив, можно разместить там, где это необходимо службам.

– **NFV**, базовая сеть IMT-2020 которой предполагает, что NF реализуются как виртуальные функции для лучшего управления ресурсами и экономии затрат. NFV, разделяющая аппаратное и программное обеспечение, делает сеть более гибкой и упрощает ее, сводя к минимуму зависимость от ограничений аппаратуры.

– **Сетевой сегмент**, целью которого является поддержка нескольких типов услуг в общей физической сетевой инфраструктуре. Это позволяет предоставлять настраиваемые сквозные сети для удовлетворения различных требований. Каждый сетевой сегмент может содержать различные NF в соответствии с требованиями к услугам.

## I.5 Плоскость управления

Плоскость управления отвечает за управление сетью и оркестровку служб. Чтобы управлять сетями и контролировать их, плоскость управления подключается к сети доступа, базовой сети и SDN через отдельный выделенный канал связи, как показано на рисунке I.5. Управление сетью заключается как минимум в выполнении следующих функций: управление ошибками (FM), управление рабочими характеристиками (PM), управление конфигурацией (CM) и управление трассировкой (TM). Помимо этих функций управления сетью необходимы также следующие функции для управления сетевым сегментом: управление жизненным циклом сегмента, управление возможностями сегмента и обнаружение сетевых ресурсов. В оркестровке служб применяются гибкие механизмы контроля и управления ресурсами для предоставления, управления и повторной оптимизации сетевых служб.

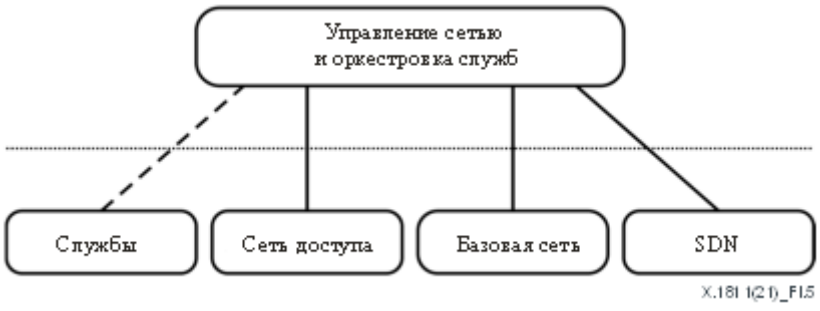


**Рисунок I.5 – Общая архитектура управления**

# Дополнение II

## Криптографические алгоритмы с несимметричным ключом, обеспечивающие квантовую безопасность

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В данном Дополнении перечислены хорошо известные криптографические алгоритмы с несимметричным ключом**,** обеспечивающие квантовую безопасность.

### II.1 Алгоритмы на основе решеток

Некоторые алгоритмы на основе решеток:

– усеченное кольцо многочленов *N*-й степени (NTRU) [b-Hoffstein];

– обучение с ошибками (LWE) [b-Regev];

– обучение с ошибками в кольце (R-LWE) [b-Lyubashevsky];

– схема NewHope [b-Alkim].

### II.2 Алгоритмы на основе хеширования

Некоторые алгоритмы на основе хеширования:

– расширенная схема подписи Меркла (XMSS) [b-Buchmann];

– SPHINCS [b-Bernstein 2015];

– подписи на основе хеширования Лейтона – Микали (LMS) [b-IRTF RFC 8554].

### II.3 Алгоритмы на основе кодирования

Некоторые алгоритмы на основе кодирования:

– классический алгоритм Мак-Элиса [b-McEliece];

– Схема Нидеррейтера [b-Dinh].

### II.4 Многомерные алгоритмы

Некоторые практические схемы подписи, основанные на многомерных алгоритмах:

– Схема Rainbow [b-Ding];

– "несбалансированная схема масла и уксуса" (UOV) [b-Kipnis].

### II.5 Стандартизация постквантовой криптографии NIST

20 декабря 2016 года NIST объявил запрос на представление кандидатов на роль постквантовых криптографических алгоритмов с открытым ключом. По итогам первого раунда NIST принял 69 схем-кандидатов, в числе которых было 20 схем цифровой подписи и 49 механизмов шифрования с открытым ключом (PKE) или механизмов инкапсуляции ключей (KEM). 30 января 2019 года NIST выбрал в качестве кандидатов второго раунда 26 алгоритмов, перечисленных в таблице II.1, в числе которых – девять схем цифровой подписи и 17 схем PKE и создания ключей [b-NISTIR 8240].

**Таблица II.1 – Алгоритмы второго раунда NIST**

| Классификация | База задач | Алгоритм |
|---|---|---|
| Шифрование/KEM | На основе решетки | Crystals-Kyber |
| | | FrodoKEM |
| | | LAC |
| | | NewHope |
| | | NTRU |
| | | NTRU Prime |
| | | Round 5 |
| | | Saber |
| | | Three Bears |
| | На основе кода | Классический алгоритм Мак-Элиса |
| | | NTS-KEM |
| | | BIKE |
| | | HQC |
| | | Rollo |
| | | LEDAcrypt |
| | | RQC |
| | На основе изогенности | SIKE |
| Подпись | На основе решетки | Crystals-Dilithium |
| | | Falcon |
| | | qTesla |
| | На основе многомерности | GeMSS |
| | | LUOV |
| | | MQDSS |
| | | Rainbow |
| | На основе хеширования | Sphincs+ |
| | | Picnic |

NIST намерен стандартизировать постквантовые алгоритмы с открытым ключом для использования в широком спектре протоколов, таких как TLS, защищенный командный процессор (SSH), обмен ключами по интернету (IKE), IPsec и расширения безопасности системы доменных имен (DNSSec) [b-NISTIR 8240].

NIST оценивает алгоритмы второго раунда как с точки зрения безопасности, так и с точки зрения быстродействия. Схема шифрования NTRU была изобретена в 1996 году, и степень ее безопасности достаточно хорошо изучена и исследована на протяжении десятилетий. Кроме того, схема шифрования NTRU стандартизирована в [b-IEEE Std 1363.1]. Классическая схема Мак-Элиса основана на алгоритме [b-McEliece], который не был взломан и считается безопасным в мире квантовых вычислений. Многие же другие схемы появились не более 10 лет назад. Таким образом, эти схемы все еще нуждаются в глубоком криптоанализе со стороны криптографического сообщества, чтобы укрепить уверенность в их безопасности. В частности, схема SIKE, впервые опубликованная в [b-Jao], основана на задаче нахождения изогений между суперсингулярными эллиптическими кривыми, которая не изучена в такой степени, как некоторые задачи обеспечения безопасности, связанные с другими кандидатами [b-NISTIR 8240].

Совершенная прямая секретность означает, что, даже если раскрыт долговременный ключ, ключи прошлых сеансов раскрыты не будут. Это полезное свойство защиты, необходимое для широко

используемых протоколов безопасности, таких как IPsec и TLS. Из всех кандидатов совершенную прямую секретность способны обеспечить только схемы SIKE и NewHope.

Быстродействие алгоритмов измеряется размером открытых ключей, зашифрованного текста и подписей, а также вычислительной эффективностью шифрования и дешифрования. В алгоритмах PQC открытые ключи, зашифрованный текст и подписи обычно бывают гораздо большего размера, чем в классических алгоритмах с открытым ключом. Согласно [b-NIST PQC], размер открытого ключа алгоритмов-кандидатов варьирует от 726 байтов до более 1 Мбайта. Схема SIKE имеет наименьший размер открытого ключа, в то время как у классических схем Мак-Элиса и NTS-KEM размер открытого ключа намного больше, чем у других схем. Однако классические схемы Мак-Элиса и NTS-KEM могут с конкурентоспособной скоростью шифрования генерировать более компактный зашифрованный текст, чем другие схемы. Несмотря на наименьший размер открытого ключа, похоже, что быстродействие схемы SIKE на порядок ниже, чем у многих других кандидатов. Поэтому при выборе алгоритмов PQC необходим компромисс между эффективностью использования полосы пропускания и эффективностью вычислений.

В 2020 году NIST планирует выбрать либо кандидатов для последнего раунда, либо небольшое количество кандидатов на стандартизацию [b-NISTIR 8240]. Это означает, что будет стандартизирован не один, а несколько алгоритмов PQC. В системах подвижной связи быстродействие имеет решающее значение ввиду ценности ресурсов радиоинтерфейса и ограниченных вычислительных возможностей устройств. В системы IMT-2020 должны быть внедрены окончательные стандартизованные алгоритмы с меньшими размерами открытых ключей и зашифрованного текста и с конкурентоспособной скоростью шифрования.

# Дополнение III

## Влияние квантовых вычислений на широко распространенные криптографические алгоритмы

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В данном Дополнении показано влияние квантовых вычислений на широко распространенные криптографические алгоритмы.

В таблице III.1 приведен краткий обзор влияния мощных квантовых компьютеров на распространенные криптографические алгоритмы, такие как RSA и усовершенствованный стандарт шифрования (AES).

Неизвестно, как далеко могут продвинуться эти преимущества квантовых вычислений и насколько велик разрыв между осуществимостью классической и квантовой моделей [b-NISTIR 8105].

**Таблица III.1 – Влияние квантовых компьютеров на широко распространенные криптографические алгоритмы**
[b-NISTIR Quantum report]

| Криптографический алгоритм | Тип | Назначение | Влияние |
|---|---|---|---|
| AES | Симметрич-ный | Шифрование | Требуются ключи большого размера |
| SHA-2, SHA-3 | Хеш | Хеш-функция | Требуется выходной код большего размера |
| RSA | С открытым ключом | Подпись, транспортировка ключей | Больше не безопасный |
| ECDSA, ECDH | С открытым ключом | Подпись, обмен ключами | Больше не безопасный |
| DSA | С открытым ключом | Подпись, обмен ключами | Больше не безопасный |

# Дополнение IV

## Критерии оценки криптографической схемы, обеспечивающей квантовую безопасность

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В данном Дополнении представлены критерии оценки NIST для выбора криптографической схемы, обеспечивающей квантовую безопасность.

Представленные криптографические алгоритмы оцениваются по трем соответствующим аспектам – безопасности, стоимости, характеристикам алгоритма и его реализации [b-NIST-Sub].

### IV.1 Безопасность

Наиболее важным фактором при оценке является уровень безопасности, обеспечиваемый криптографической схемой. Схемы оцениваются по следующим признакам.

**Приложения криптографической схемы с открытым ключом.** Будут стандартизированы постквантовые алгоритмы для существующих стандартов цифровых подписей (FIPS 186) и создания ключей (SP 800-56A, SP 800-56B). Они используются в самых разных интернет-протоколах, таких как TLS, SSH, IKE, IPsec и DNSSec. Схемы оцениваются по безопасности, которую они обеспечивают в этих приложениях в процессе оценки. Заявленные приложения будут оцениваться на предмет их практической значимости, если эта оценка будет необходима для принятия решения о том, какие алгоритмы стандартизировать.

**Определение безопасности для шифрования/создания ключей.** Постквантовые алгоритмы шифрования или создания ключей должны быть "семантически безопасными" по отношению к адаптивно выбранным криптографическим атакам. В научной литературе это свойство обычно обозначают как безопасность *IND-CCA2*.

Приведенное выше определение безопасности следует рассматривать как заявление о том, что именно NIST будет считать релевантной атакой. Представленные KEM и схемы шифрования будут оцениваться по тому, насколько хорошо они, как представляется, обеспечивают это свойство при использовании в соответствии с указаниями заявителя. Заявители не обязаны представлять доказательства безопасности, хотя такие доказательства рассматриваются, если они представлены.

Для оценки уровня безопасности можно предположить, что злоумышленник имеет доступ к дешифровке не более чем $2^{64}$ выбранных шифрованных текстов; однако могут быть также рассмотрены и атаки с использованием большего количества зашифрованных текстов.

**Определение безопасности для кратковременного шифрования/создания ключей.** Хотя обеспечение безопасности выбранного зашифрованного текста необходимо для многих существующих приложений (например, протоколов обмена номинально кратковременными ключами, допускающих кеширование ключей), протокол обмена кратковременными ключами можно реализовать таким образом, что от элемента шифрования или KEM потребуется только пассивная защита.

Для этих приложений постквантовые алгоритмы для кратковременного шифрования/создания ключей должны обеспечивать семантическую безопасность по отношению к выбранным атакам с использованием открытого текста. В научной литературе это свойство обычно обозначают как безопасность *IND-CPA*.

Представленные KEM и схемы шифрования будут оцениваться по тому, насколько хорошо они, как представляется, обеспечивают это свойство при использовании в соответствии с указаниями заявителя. Заявители не обязаны представлять доказательства безопасности, хотя такие доказательства рассматриваются, если они представлены. Любые уязвимости безопасности, возникающие в результате повторного использования ключа, должны быть полностью объяснены.

**Определение безопасности для цифровых подписей.** Постквантовые алгоритмы цифровой подписи обеспечивают экзистенциально не поддающиеся фальсификации цифровые подписи по отношению к атаке с адаптивно выбранными сообщениями. В научной литературе это свойство обычно обозначают как безопасность *EUF-CMA*.

Представленные алгоритмы будут оцениваться по тому, насколько хорошо они, как представляется, обеспечивают это свойство при использовании в соответствии с указаниями заявителя.

Для оценки уровня безопасности можно предположить, что злоумышленник имеет доступ к подписям не более чем $2^{64}$ выбранных сообщений.

**Дополнительные свойства безопасности.** Хотя перечисленные выше определения безопасности охватывают многие сценарии атак, которые используются при оценке представленных алгоритмов, есть несколько других свойств, которые считаются желательными.

Одно из таких свойств – совершенная прямая секретность. Хотя это свойство можно получить с помощью стандартных функций шифрования и подписи, в некоторых случаях его стоимость может оказаться непомерно высокой. В частности, схемы шифрования с открытым ключом с алгоритмом медленной выработки ключей, такие как RSA, обычно считаются неподходящими для совершенной прямой секретности. Это тот случай, когда присутствует высокая корреляция между стоимостью и практической безопасностью алгоритма.

Другой случай взаимосвязи безопасности и производительности – стойкость к атакам по побочным каналам. Схемы, которые с минимальными затратами можно сделать устойчивыми к атакам по побочным каналам, предпочтительнее схем, производительность которых серьезно страдает при любой попытке противостоять атакам по побочным каналам. Следует отметить также, что более значимы оптимизированные реализации, направленные на защиту от атак по побочным каналам (например, реализации с постоянным временем).

Третье желательное свойство – стойкость к атакам на несколько ключей. В идеале злоумышленник не должен получать преимущества, атакуя сразу несколько ключей, независимо от того, состоит ли его цель во взломе одной пары или большого количества ключей.

Последним желательным, хотя и нечетко определенным, свойством является стойкость к неправильному применению. В идеале отдельные ошибки кодирования, сбои генератора случайных чисел, повторное использование одноразовых паролей или пар ключей (при кратковременном шифровании/создании ключей) и т. д. не должны приводить к катастрофическим последствиям.

**Другие рассматриваемые факторы.** Поскольку криптография с открытым ключом обычно подразумевает тонкую математическую структуру, очень важно, чтобы эта математическая структура была достаточно хорошо понятна, обеспечивая уверенность в безопасности криптосистемы. Для оценки этого свойства будет рассматриваться ряд факторов. При прочих равных условиях простые схемы, как правило, понятнее сложных. Точно так же схемы, принципы разработки которых могут быть связаны с зарекомендовавшими себя соответствующими исследованиями, как правило, понятнее абсолютно новых схем или схем, разработанных путем многократного исправления старых схем, оказавшихся уязвимыми для криптоанализа.

Рассматривается ясность документации схемы и качество анализа, представленного заявителем. Четкий и тщательный анализ поможет повысить качество и зрелость анализа силами более широкого сообщества. Рассматриваются любые аргументы или доказательства безопасности, предоставленные заявителем. Хотя доказательства безопасности обычно основаны на недоказанных предположениях, они часто позволяют исключить общие классы атак или связать безопасность новой схемы с известной и лучше изученной вычислительной задачей.

### IV.2 Стоимость

Стоимость криптосистемы с открытым ключом можно измерять по разным параметрам.

**Размер открытого ключа, зашифрованного текста и подписи.** Схемы оцениваются по размерам создаваемых ими открытых ключей, шифрованных текстов и подписей. Все это может служить важным учитываемым фактором для приложений с ограниченной полосой пропускания или интернет-протоколов с ограниченным размером пакетов. Степень важности размера открытого ключа может варьировать в зависимости от приложения; если приложения способны кешировать открытые ключи или иным образом избегать их частой передачи, значение размера открытого ключа может быть меньше. Напротив, для приложений, в которых совершенная прямая секретность достигается путем передачи нового открытого ключа в начале каждого сеанса, вероятно, выгоднее использовать алгоритмы с относительно короткими открытыми ключами.

**Вычислительная эффективность операций с открытыми и секретными ключами.** Схемы оцениваются также по вычислительной эффективности операций с открытыми ключами (шифрование, инкапсуляция и проверка подписи) и секретными ключами (дешифрование, декапсуляция и подписание). Вычислительные затраты на эти операции оцениваются с точки зрения как аппаратного, так и программного обеспечения. Почти во всех случаях важны вычислительные затраты на операции как с открытыми, так и с секретными ключами, но некоторые приложения могут быть более чувствительными к тем или другим. Например, операции подписания или дешифрования могут выполняться устройством с ограниченными вычислительными возможностями, таким как смарт-карта, или, напротив, сервером, обрабатывающим большой объем трафика, которому придется потратить значительную часть своих вычислительных ресурсов на проверку подписей клиентов.

**Вычислительная эффективность выработки ключей.** В соответствующих случаях схемы также оцениваются по вычислительной эффективности операций по выработке ключей. Наиболее распространенным сценарием, в котором важно время выработки ключей, является использование алгоритма шифрования с открытым ключом или KEM для обеспечения совершенной прямой секретности. Тем не менее возможно, что в некоторых приложениях время выработки ключей окажется важным и для схем цифровой подписи.

**Отказы при дешифровании.** Некоторые алгоритмы шифрования с открытым ключом и KEM даже при правильной реализации иногда создают зашифрованные тексты, которые невозможно расшифровать/декапсулировать. Для большинства приложений важно, чтобы такие отказы при дешифровании были редкими или отсутствовали. Для алгоритмов с возможностью отказов дешифрования/декапсуляции заявители должны указать частоту отказов, а также анализ их возможного влияния на безопасность. Хотя приложения всегда могут получить приемлемо низкую частоту отказов при дешифровании за счет многократного шифрования одного и того же открытого текста, а при отказе при создании ключа просто перезапускать интерактивные протоколы, подобные решения имеют собственные эксплуатационные расходы.

### IV.3 Характеристики алгоритма и реализации

**Гибкость.** При условии хорошей общей безопасности и производительности более гибкие схемы будут соответствовать потребностям большего числа пользователей, чем менее гибкие, и поэтому являются предпочтительными.

К некоторым примерам "гибкости", в частности, можно отнести следующие.

1 В схемы можно внести изменения для обеспечения дополнительных функций, выходящих за рамки минимальных требований шифрования с открытым ключом, KEM (механизма инкапсуляции ключей) или цифровой подписи (например, асинхронный или неявно аутентифицированный обмен ключами и т. д.).

2 Параметры схемы легко настраиваются для решения ряда задач повышения безопасности и производительности.

3 Алгоритмы могут быть безопасно и эффективно реализованы на самых разных платформах, включая ограниченные, такие как смарт-карты.

4 Реализации алгоритмов можно распараллелить для достижения более высокой производительности.

5 Схемы можно включить в существующие протоколы и приложения с минимально возможным количеством изменений.

**Простота.** Схемы оцениваются по относительной простоте конструкции.

**Внедрение.** В процессе оценки рассматриваются факторы, которые могут препятствовать или способствовать широкому внедрению алгоритма или реализации, включая, помимо прочего, интеллектуальную собственность, охватывающую алгоритм или реализацию, и наличие и условия лицензий для заинтересованных сторон. Рассматриваются заверения, содержащиеся в заявлениях их подателей и любых обладателей патентов, причем значительное предпочтение отдается тем из них, в которых содержатся обязательства по лицензированию без компенсации на разумных условиях и явно провозглашается отсутствие несправедливой дискриминации.

## Библиография


[b-ITU-T X.1196] Recommendation ITU-T X.1196 (2012), *Framework for the downloadable service and content protection system in the mobile Internet Protocol television environment*.

[ITU-T X.1197] Recommendation ITU-T X.1197 (2019), *Guidelines on the selection of cryptographic algorithms for IPTV services, Amendment 1*.

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 год), *Базовые термины и определения в области управления определением идентичности*.

[b-ITU-T X.1254] Рекомендация МСЭ-Т X.1254 (2012 год), *Структура гарантии аутентификации объекта*.

[b-ITU-T Y.2014] Recommendation ITU-T Y.2014 (2008), *Network attachment control functions in next generation networks*.

[b-ETSI 135 205] ETSI 135 205 V4.0.0 (2001), *Universal mobile telecommunications system (UMTS); LTE;3G security*; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General.

[b-ETSI 135 231] ETSI 135 231 V12.1.0 (2014), *Universal mobile telecommunications system (UMTS)*; LTE; Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification.

[b-ETSI GR QSC 004] ETSI GR QSC 004 V1.1.1 (2017), *Quantum-safe cryptography; Quantum-safe threat assessment*.

[b-ETSI GR QSC 006] ETSI GR QSC 006 V1.1.1 (2017), *Quantum-safe cryptography (QSC); Limits to quantum computing applied to symmetric key sizes*.

[b-ETSI GS NFV 002] ETSI GS NFV 002 V1.1.1 (2013). *Network functions virtualisation (NFV); Architectural framework*.

[b-ETSI GS NFV-SEC 012] ETSI GS NFV-SEC 012 V3.1.1 (2017), *Network functions virtualisation (NFV) release 3;Security; System architecture specification for execution of sensitive NFV components*.

[b-ETSI GS NFV-SEC 014] ETSI GS NFV-SEC 014 V3.1.1 (2018), *Network functions virtualisation (NFV) release 3; NFV security; Security specification for MANO components and reference points*.

[b-3GPP TS 33.210] 3GPP TS 33.210 V16.2.0 (2019), *3G security; Network domain security (NDS); IP network layer security*.

[b-3GPP TS 33.220] 3GPP TS 33.220, V16.0.0 (2019), *Generic authentication architecture (GAA); generic bootstrapping architecture (GBA)*.

[b-3GPP TS 33.310] 3GPP TS 33.310 V16.2.0 (2019), *Network domain security (NDS); Authentication framework (AF)*.

[b-3GPP TS 33.501] 3GPP TS 33.501, version 16.1.0 (2019), *System architecture for the 5G system*.

[b-3GPP TR 33.841] 3GPP TR 33.841 (2018), *Study on the support of 256-bit algorithms for 5G*.

[b-Häner] Häner, T., Roetteler, M., Svore, K.M. (2017). Factoring using 2*n* + 2 qubits with Toffoli based modular multiplication. *Quantum Information and Computation*, **18**(7-8), pp. 673-684.

[b-Hoffstein] Hoffstein, J., Pipher, J., Silverman, J.H. (1998). NTRU: A ring-based public key cryptosystem. In: Buhler, J.P. (editor), *Algorithmic number theory – ANTS 1998*, pp. 267-288. *Lecture Notes in Computer Science*, volume. 1423. Berlin: Springer.DOI: 10.1007/BFb0054868.

[b-IEEE Std 1363.1] IEEE Std 1363.1-2008, *IEEE Standard Specification for public key cryptographic techniques based on hard problems over lattices*.

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-hashing for message authentication*.

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-shared key ciphersuites for transport layer security (TLS)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security architecture for the Internet protocol*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP encapsulating security payload (ESP)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet key exchange (IKEv2) protocol*.

[b-IETF RFC 4492] IETF RFC 4492 (2006), *Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS)*.

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic algorithm implementation requirements for encapsulating security payload (ESP) and authentication header (AH)*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5288] IETF RFC 5288 (2008), *AES Galois counter mode (GCM) cipher suites for TLS*.

[b-IETF RFC 5289] IETF RFC 5289 (2008), *TLS elliptic curve cipher suites with SHA-256/384 and AES Galois counter mode (GCM)*.

[b-IETF RFC 5869] IETF RFC 5869 (2010), *HMAC-based extract-and-expand key derivation function (HKDF)*.

[b-IETF RFC 6083] IETF RFC 6083 (2011), *Datagram transport layer security (DTLS) for stream control transmission protocol (SCTP)*.

[b-IETF RFC 6347] IETF RFC 6347 (2012), *Datagram transport layer security version 1.2*.

[b-IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 authorization framework*.

[b-IETF RFC 7296] IETF RFC 7296 (2014), *Internet key exchange protocol version 2 (IKEv2)*.

[b-IETF RFC 7515] IETF RFC 7515 (2015), *JSON web signature (JWS)*.

[b-IETF RFC 7516] IETF RFC 7516 (2015), *JSON web encryption (JWE)*.

[b-IETF RFC 7519] IETF RFC 7519 (2015), *JSON web token (JWT)*.

[b-IRTF RFC 8554] IRTF RFC 8554 (2019), *Leighton-Micali hash-based signatures*.

[b-ISO 7498-2] ISO 7498-2:1989, *Information Processing Systems* – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.

[b-ISO/IEC TR 22417] ISO/IEC TR 22417:2017, *Information technology* – Internet of things (IoT) use cases.

[b-Ajtai] Ajtai, M. (1998). The shortest vector problem in $L_2$ is NP-hard for randomized reductions (extended abstract). In: Vitter, J. (editor). *STOC '98: Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pp 10–19. New York, NY: Association for Computing Machinery. DOI: 10.1145/276698.276705.

[b-Alkim] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P. (2017). Post-quantum key exchange – A new hope, *Cryptology ePrint Archive*, Report 2015/1092. Available [viewed 2020-02-03] at: https://eprint.iacr.org/2015/1092.

[b-Amy] Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., Schanck, J. (2017). Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. In: Avanzi, R., Heys H. (editors). *Selected areas in cryptography, SAC 2016*, St. Johns, Canada, 2016, pp. 317-337. *Lecture*

*Notes in Computer Science*, volume 10532. Cham: Springer. DOI: 10.1007/978-3-319-69453-5_18.

[b-Banchi] Banchi, L., Pancotti, N., Bose, S. (2016). Quantum gate learning in qubit networks: Toffoli gate without time-dependent control. *npj Quantum Information* **2**, 16019. DOI: 10.1038/npjqi.2016.19. Available [viewed 2020-02-02] at: https://www.nature.com/articles/npjqi201619#ref-link-section-82.

[b-Bertoni] Betrtoni, G., Daemen, J., Peeters, M., Van Assche, G. *Keccak sponge function family main document*. Available at: https://keccak.team/obsolete/Keccak-main-1.1.pdf.

[b-Bernstein 2009] Bernstein, D.J. (2009). Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? In: Workshop Record of SHARCS '09: Special-purpose Hardware for Attacking Cryptographic Systems. Available [viewed 2020-02-03] at: https://cr.yp.to/hash/collisioncost-20090517.pdf.

[b-Bernstein 2015] Bernstein, D.J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., Wilcox-O'Hearn, Z. (2015). SPHINCS: Practical stateless hash-based signatures. In: Oswald, E., Fischlin, M. (editors). *Advances in Cryptology – EUROCRYPT 2015*, pp. 368-397. *Lecture Notes in Computer Science*, volume 9056. Berlin: Springer. DOI: 10.1007/978-3-662-46800-5_15.

[b-Buchmann] Buchmann, J., Dahmen, E., Hülsing, A. (2011). XMSS: A practical forward secure signature scheme based on minimal security assumptions. In: Yang, B.-Y. (editor). *Post-quantum cryptography*, pp. 117-129. *Lecture Notes in Computer Science*, volume 7071. Berlin: Springer. DOI: 10.1007/978-3-642-25405-5_8.

[b-CSA] Cloud Security Alliance (2017), *Applied quantum-safe security: Quantum-resistant algorithms and quantum key distribution.* Available [viewed 2020-02-03] from: https://cloudsecurityalliance.org/download/applied-quantum-safe-security.

[b-Dinh] Dinh, H., Moore, C., Russell, A. (2011). McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks. In: Rogaway, P. (editor). *Advances in cryptology – CRYPTO 2011*, pp. 761-779. *Lecture Notes in Computer Science*, volume 6841. Berlin: Springer. DOI: 10.1007/978-3-642-22792-9_43.

[b-Ding] Ding, J. Schmidt, D. (2005). Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (editors). *Applied Cryptography and Network Security, ACNS 2005*, pp. 164-175. *Lecture Notes in Computer Science*, volume 3531. Berlin: Springer. DOI: 10.1007/11496137_12.

[b-Fowler] Fowler, A.G., Mariantoni, M., Martinis, J.M., Cleland, A.N. (2012). Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, **86**, 032324. DOI: 10.1103/PhysRevA.86.032324. Available [viewed 2020-02-02] at: https://web.physics.ucsb.edu/~martinisgroup/papers/Fowler2012.pdf.

[b-Garey] Garey, M.R. Johnson, D.S. (1979). *Computers and intractability: A guide to the theory of NP-completeness*. New York, NY: W.H. Freeman. 338 pp.

[b-Grassl] Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In: Takagi T. (editor). *Post-quantum cryptography – PQCrypto 2016*, pp. 29-43. *Lecture Notes in Computer Science*, volume 9606. Cham: Springer. Available [viewed 2020-02-03] at: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/04/1512.04965-1.pdf.

[b-Grover] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. In: *STOC '96: Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pp 212-219. New York, NY: Association for Computing Machinery. DOI: 10.1145/237814.237866.

[b-Jao] Jao, D., De Feo, L. (2011), Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B-Y. (editor). *Post-quantum cryptography*, pp 19-34. *Lecture Notes in Computer Science*, volume 7071. Berlin: Springer. DOI: 10.1007/978-3-642-25405-5_2.

[b-Kipnis] Kipnis, A., Patarin, J., Goubin, L. (1999), Unbalanced oil and vinegar signature schemes. In: Stern, J. (editor). *Advances in Cryptology – EUROCRYPT '99*. pp. 206-222. *Lecture Notes in Computer Science*, volume 1592. Berlin: Springer. DOI: 10.1007/3-540-48910-X_15.

[b-Lyubashevsky] Lyubashevsky, V., Peikert, C., Regev, O. (2013), On ideal lattices and learning with errors over rings. *Journal of the ACM*, **60**(6), Article No. 43. DOI: 10.1145/2535925.

[b-McEliece] McEliece, R.J. (1978), A *public-key cryptosystem based on algebraic coding theory*. In: *DSN Progress Report*, No. 44, pp. 114–116. Bibcode:1978DSNPR. Available [viewed 2020-02-03] at: https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

[b-Moody] Moody, D. (2019), *NIST status update on elliptic curves and post-quantum crypto*. Gaithersberg, MA: National Institute of Standards and Technology. 20 pp. Available [viewed 2020-02-03] at: https://csrc.nist.gov/CSRC/media/Presentations/NIST-Status-Update-on-Elliptic-Curves-and-Post-Qua/images-media/moody-dustin-threshold-crypto-workshop-March-2019.pdf.

[b-Moses] Moses, T. (2009), *Quantum computing and cryptography – Their impact on cryptographic practice*. Minneapolis, MN: Entrust Inc. 12 pp. Available [viewed 2020-02-03] at: https://www.entrust.com/wp-content/uploads/2013/05/WP_QuantumCrypto_Jan09.pdf.

[b-NASEM] National Academies of Sciences, Engineering, and Medicine (2018). *Quantum computing: Progress and prospects*. Washington, DC: National Academies Press. 272 pp. DOI: 10.17226/25196.

[b-NIST FIPS 186-4] National Institute of Standards and Technology Federal Information Processing Standard 186-4 (2013), *Digital signature standard (DSS)*. DOI: 10.6028/NIST.FIPS.186-4. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[b-NIST FIPS 197] National Institute of Standards and Technology Federal Information Processing Standard 197 (2001), *Specification for the advanced encryption standard (AES)*. Available [viewed 2020-02-14] at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[b-NISTIR 8105] National Institute of Standards and Technology Internal Report 8105 (2016), *Report on* post-*quantum cryptography*. Gaithersberg, MA: National Institute of Standards and Technology. 15 pp. DOI: 10.6028/NIST.IR.8105. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[b-NISTIR 8240] National Institute of Standards and Technology Internal Report 8240 (2019), *Status* report on the first round of *the NIST post-quantum cryptography standardization process*. Gaithersberg, MA: National Institute of Standards and Technology. 27 pp. DOI: 10.6028/NIST.IR.8240. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf.

[b-NIST PQC] National Institute of Standards and Technology Post-Quantum Cryptography: Round 2 – algorithm comparison. Available [viewed 2020-02-14] at:http://hdc.amongbytes.com/post/20190130-pqc-round2/.

[b-NIST SP 800-38B] National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for block cipher modes of operation: The CMAC mode for authentication*. Gaithersberg, MA: National Institute of Standards and Technology. 21 pp. DOI: 10.6028/NIST.SP.800-38B. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf.

[b-NIST SP 800-67] National Institute of Standards and Technology Special Publication 800-67 Rev. 2 (2017), *Recommendation for the triple data encryption algorithm (TDEA) block cipher*. DOI: 10.6028/NIST.SP.800-67r2.

[b-NIST-Sub] National Institute of Standards and Technology. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. Available [viewed 2020-03-20] at : https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[b-ONF TR-511] Open Network Foundation Technical Recommendation 511 (2015), *Principles and practices for securing software-defined networks*. Available [viewed 2020-02-02] at: https://www.opennetworking.org/wp-content/uploads/2014/10/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf.

[b-QC1] IBM's processor pushes quantum computing closer to 'supremacy' available at: https://www.engadget.com/2017/11/10/ibm-50-qubit-quantum-computer/.

[b-QC2] Practical Quantum Computers, available at: https://www.technologyreview.com/s/603495/10-breakthrough-technologies-2017-practical-quantum-computers/.

[b-Regev] Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. In: *STOC'05 Proceedings of the 37th Annual ACM Symposium on Theory of Computing*. pp. 84-93. New York, NY: Association for Computing Machinery. DOI: 10.1145/1060590.1060603.

[b-Roetteler] Roetteler, M., Naehrig, M., Krysta M. Svore, K.M., Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. In: Takagi T., Peyrin T. (editors). *Advances in Cryptology – ASIACRYPT 2017*, pp. 241-270. *Lecture Notes in Computer Science*, volume 10625. Cham: Springer. DOI: 10.1007/978-3-319-70697-9_9. Available [viewed 2020-02-02] at: https://www.microsoft.com/en-us/research/wp-content/uploads/2017/09/1706.06752.pdf.

[b-Schneier] Schneier, B. (1994). The Blowfish encryption algorithm. *Dr. Dobb's Journal*, 19(4), pp. 38-40. Available [viewed 2020-02-03] from: https://www.drdobbs.com/security/the-blowfish-encryption-algorithm/184409216.

[b-Shor 1997] Shor, P.W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), pp. 1484–1509. DOI: 10.1137/S0097539795293172.

[b-Shor 1999] Shor, P.W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev*. 41(2), pp. 303-332. DOI: 10.1137/S0036144598347011.

## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

| | |
|---|---|
| Серия A | Организация работы МСЭ-Т |
| Серия D | Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ |
| Серия E | Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы |
| Серия F | Нетелефонные службы электросвязи |
| Серия G | Системы и среда передачи, цифровые системы и сети |
| Серия H | Аудиовизуальные и мультимедийные системы |
| Серия I | Цифровая сеть с интеграцией служб |
| Серия J | Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов |
| Серия K | Защита от помех |
| Серия L | Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений |
| Серия M | Управление электросвязью, включая СУЭ и техническое обслуживание сетей |
| Серия N | Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ |
| Серия O | Требования к измерительной аппаратуре |
| Серия P | Качество телефонной передачи, телефонные установки, сети местных линий |
| Серия Q | Коммутация и сигнализация, а также соответствующие измерения и испытания |
| Серия R | Телеграфная передача |
| Серия S | Оконечное оборудование для телеграфных служб |
| Серия T | Оконечное оборудование для телематических служб |
| Серия U | Телеграфная коммутация |
| Серия V | Передача данных по телефонной сети |
| **Серия X** | **Сети передачи данных, взаимосвязь открытых систем и безопасность** |
| Серия Y | Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города |
| Серия Z | Языки и общие аспекты программного обеспечения для систем электросвязи |

Отпечатано в Швейцарии,
Женева, 2021 г.