Международный союз электросвязи

МСЭ-Т X.1364

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(03/2020)

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

Безопасные приложения и услуги (2) – Безопасность интернета вещей (IoT)

Требования безопасности и структура безопасности узкополосного интернета вещей

Рекомендация МСЭ-Т X.1364

Международный союз электросвязи

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 распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного 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	X.1700–X.1729

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

Рекомендация МСЭ-Т X.1364

Требования безопасности и структура безопасности узкополосного интернета вещей

Резюме

Рекомендация МСЭ-Т X.1364 ставит целью проанализировать возможные схемы развертывания и типовые сценарии применения узкополосного интернета вещей (NB-IoT). В ней определяются угрозы и требования безопасности, характерные для развертывания NB-IoT, и таким образом создается структура мер безопасности, с помощью которой оператор может обеспечить защиту применений этой новой технологии NB-IoT.

Ввиду текущих тенденций развития технологии электросвязи изменяется характер подвижной связи – на смену связи человека с человеком приходит связь человека с вещью и даже вещи с вещью. Закономерным результатом такой эволюции становится интернет вещей.

В сравнении с технологиями ближней связи, такими, например, как Bluetooth и ZigBee, сети сотовой связи характеризуются обширным покрытием, мобильностью и возможностью установки большого числа соединений, что может обеспечить большее разнообразие сценариев применения. Поэтому, как предполагается, они станут основной технологией соединений в интернете вещей.

NB-IoT функционирует на базе технологии сетей сотовой подвижной связи, которая использует ширину полосы пропускания лишь порядка 180 кГц. Он может быть развернут непосредственно на основе сетей глобальной системы подвижной связи (GSM), универсальной системы подвижной электросвязи (UMTS) или на основе сетей на базе технологии долгосрочного развития (LTE) для снижения затрат и обеспечения бесшовного обновления.

Ожидается, что благодаря своему низкому уровню рассеиваемой мощности, обширному покрытию, низкой стоимости и высокой пропускной способности NB-IoT получит значительное распространение среди операторов и широкое применение в различных вертикальных отраслях.

Так как технология NB-IoT новая, у нее есть особенности, которые могут обусловить новые проблемы безопасности. Чтобы обеспечить безопасность развертывания NB-IoT и его приложений, необходимо проанализировать угрозы и соответствующие требования безопасности, характерные для NB-IoT, а также создать общую структуру безопасности NB-IoT.

Хронологическая справка

Издание	Рекомендация	Утверждена	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1364	26.03.2020 года	17-я	11.1002/1000/14088

Ключевые слова

Интернет вещей, структура, требования безопасности, узкополосный.

---

* Для доступа к Рекомендации наберите URL http://handle.itu.int/ в вашем веб-браузере, а затем 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 с целью 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

Рекомендация МСЭ-Т X.1364

Требования безопасности и структура безопасности узкополосного интернета вещей

1 Сфера применения

В настоящей Рекомендации анализируются возможные схемы развертывания и типовые сценарии применения узкополосного интернета вещей (NB-IoT). В ней определяются угрозы и требования безопасности, характерные для реализаций NB-IoT, и создается структура безопасности, с помощью которой оператор сможет обеспечить защиту применений этой новой технологии NB-IoT.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок 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 всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

[ETSI TS 123 401] ETSI TS 123 401 V15.8.0 (2019-10), LTE; *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 15.8.0 Release 15).*

[ETSI TS 123 501] ETSI TS 123 501 V15.6.0 (2019-10), 5G; *System architecture for the 5G System (5GS) (3GPP TS 23.501 version 15.6.0 Release 15)*

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.1141] – процесс определения того, является ли на самом деле кто-то или что-то именно тем, кем он себя объявляет с данной степенью достоверности.

3.1.2 Возможность (capability) [b-ITU-T X.1145] – возможность предоставления услуги, обеспечиваемая системой или оборудованием.

3.1.3 Сотовый IoT (cellular IoT) [ETSI TS 123 401] – сотовая сеть, поддерживающая устройства низкого уровня сложности и низкой пропускной способности для сети вещей. Сотовый IoT поддерживает оба вида трафика: IP и не-IP.

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

3.1.5 Шифрование (encryption) [b-ITU-T X.800] – криптографическое преобразование данных (см. Криптография) для создания зашифрованного текста.

ПРИМЕЧАНИЕ. – Шифрование может быть необратимым, и в этом случае выполнение соответствующего процесса дешифрования невозможно.

3.1.6 Объект (entity) [b-ITU-T X.1252] – что-либо, что существует отдельно и обособленно и может быть определено в контексте.

ПРИМЕЧАНИЕ. – Объектом может быть физическое лицо, животное, юридическое лицо, организация, активный или пассивный предмет, устройство, применение программного обеспечения, услуга и т. п. или группа таких объектов. В контексте электросвязи примерами объектов являются точки доступа, абоненты, пользователи, сетевые элементы, сети, применения программного обеспечения, услуги и устройства, интерфейсы и т. п.

3.1.7 Улучшенная базовая сеть пакетной передачи данных (evolved packet core) [b-ITU-T Q.1743] – структура для усовершенствования систем 3GPP или перехода с них на системы с более высокой скоростью передачи данных, меньшим временем задержки передачи и оптимизацией пакетов, поддерживающие множество технологий RAT.

3.1.8 Улучшенная система пакетной передачи данных (evolved packet system) [b-ITU-T Q.1743] – система, представляющая собой усовершенствованную сеть UMTS третьего поколения (3G) и характеризующаяся более высокими скоростями передачи данных, меньшим временем задержки передачи сигналов и оптимизацией пакетов с поддержкой множества RAT. Улучшенная система пакетной передачи данных состоит из улучшенной базовой сети пакетной передачи данных и улучшенной сети радиодоступа (E-UTRA и E-UTRAN).

3.1.9 Управление ключами (key management) [b-ITU-T X.800] – генерирование, хранение, распределение, удаление, архивирование и применение ключей в соответствии со стратегией безопасности.

3.1.10 Узкополосный интернет вещей (narrowband-IoT) [ETSI TS 123 401] – технология радиодоступа 3GPP, входящая в состав сотового IoT. Обеспечивает доступ к услугам сети через E-UTRA с шириной полосы частот канала, ограниченной значением 180 кГц (что соответствует одному PRB). Если в каком-либо пункте не указано иное, узкополосный интернет вещей является подмножеством E-UTRAN.

3.1.11 Угроза (threat) [b-ITU-T X.800] – потенциальное нарушение безопасности.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 Узел обслуживающего шлюза CIoT (CIoT serving gateway node (C-SGN)) – узел обслуживающего шлюза сотового интернета вещей (C-SGN) представляет собой вариант реализации улучшенной базовой сети пакетной передачи данных (EPC) с совмещенным шлюзом, который сводит к минимуму число физических объектов путем совместного размещения объектов улучшенной системы пакетной передачи данных (EPS) в трактах плоскостей управления и пользователя (например, объект управления мобильностью (MME), обслуживающий шлюз (S-GW), и шлюз сети передачи данных с коммутацией пакетов (P-GW)), что может быть предпочтительным в реализациях CIoT.

ПРИМЕЧАНИЕ. – Функции, перечисленные в настоящем определении, см. в [ETSI TS 123 401].

3.2.2 Улучшенный узел B (evolved node B (eNodeB)) – узел беспроводного доступа, на котором размещены функциональные элементы управления радиоресурсами, разуплотнения данных на линии вверх и шифрования потока пользовательских данных, маршрутизации данных плоскости пользователя и т. п.

ПРИМЕЧАНИЕ. – Функции, перечисленные в настоящем определении, см. в [ETSI TS 123 401].

3.2.3 Сеть расширенного универсального наземного радиодоступа (evolved universal terrestrial radio access network (E-UTRAN)) – сеть радиодоступа, функции которой включают сжатие заголовков и шифрование данных плоскости пользователя, выбор MME, принудительное задание скорости передачи данных на уровне носителя на линии вверх и вниз, управление допуском на уровне носителя, контроль перегрузки и т. п.

ПРИМЕЧАНИЕ. – Функции, перечисленные в настоящем определении, см. в [ETSI TS 123 401].

3.2.4 Сервер собственных абонентов (home subscriber server (HSS)) – элемент базовой сети подвижной связи, функциями которого являются хранение информации об абонентской подписке пользователя и управление этой информацией.

ПРИМЕЧАНИЕ. – Функции, перечисленные в настоящем определении, см. в [ETSI TS 123 401].

3.2.5 Объект управления мобильностью (mobility management entity (MME)) – элемент базовой сети подвижной связи, функциями которого являются управление списком зоны слежения, определение местоположения оборудования пользователей (UE), выбор обслуживающего шлюза (S-GW) и сетевого шлюза сети передачи данных с коммутацией пакетов (P-GW), выбор передачи обслуживания, аутентификация, авторизация, управление носителем и т. п.

ПРИМЕЧАНИЕ. – Функции, перечисленные в настоящем определении, см. в [ETSI TS 123 401].

3.2.6 Сетевой шлюз сети передачи данных с коммутацией пакетов (packet data network gateway (P-GW)) – элемент базовой сети подвижной связи, функциями которого являются индивидуальная фильтрация пакетов для каждого пользователя, распределение адресов протокола Интернет оборудованию пользователей, маркировка макетов на транспортном уровне, взимание платы на уровне обслуживания и т. п.

ПРИМЕЧАНИЕ. – Функции, перечисленные в настоящем определении, см. в [ETSI TS 123 401].

3.2.7 Функция предоставления возможностей обслуживания (service capability exposure function (SCEF)) – элемент базовой сети подвижной связи, функциями которого являются аутентификация и авторизация, обнаружение предоставленных возможностей по обслуживанию, управление политиками, настройка параметров сети и т. п.

ПРИМЕЧАНИЕ. – Функции, перечисленные в настоящем определении, см. в [ETSI TS 123 401].

3.2.8 Обслуживающий шлюз (*serving gateway* (S-GW)) – элемент базовой сети подвижной связи, функциями которого являются работа в качестве местной точки привязки мобильности для передачи обслуживания между узлами eNodeB, привязка мобильности при переходе между сетями 3GPP, маршрутизация и переадресация пакетов, маркировка пакетов на транспортном уровне, учет начисления платы между операторами и т. п.

ПРИМЕЧАНИЕ. – Функции, перечисленные в настоящем определении, см. в [ETSI TS 123 401].

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

3G	3rd Generation	Третье поколение
3GPP	3rd Generation Partnership Project	Проект партнерства третьего поколения
CDMA	Code Division Multiple Access	Многостанционный доступ с кодовым разделением
CIoT	Cellular Internet of Things	Сотовый интернет вещей
C-SGN	CIoT Serving Gateway Node	Узел обслуживающего шлюза CIoT
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
EPC	Evolved Packet Core	Улучшенная базовая сеть пакетной передачи данных
eNodeB	Evolved Node B	Улучшенный узел B
EPS	Evolved Packet System	Улучшенная система пакетной передачи данных
E-UTRAN	Evolved Universal Terrestrial Access Network	Сеть расширенного универсального наземного радиодоступа
GSM	Global System for Mobile Communication	Глобальная система подвижной связи
HSS	Home Subscriber Server	Сервер собственных абонентов
IMEI	International Mobile Equipment Identity	Международный идентификатор аппаратуры подвижной связи
IP	Internet Protocol	Протокол Интернет
LTE	Long Term Evolution	Технология долгосрочного развития
MME	Mobility Management Entity	Объект управления мобильностью
NB-IoT	Narrowband Internet of Things	Узкополосный интернет вещей
P-GW	Packet Data Network Gateway	Сетевой шлюз сети передачи данных с коммутацией пакетов
RAT	Radio Access Technology	Технология радиодоступа
SCEF	Service Capability Exposure Function	Функция предоставления возможностей обслуживания

S-GW	Serving Gateway	Обслуживающий шлюз
SMS	Short Message Service	Служба коротких сообщений
SIM	Subscriber Identification Module	Модуль идентификации абонента
UE	User Equipment	Оборудование пользователя
UMTS	Universal Mobile Telecommunications System	Универсальная система подвижной электросвязи
UTRA	Universal Terrestrial Radio Access	Сеть универсального наземного радиодоступа

5 Условные обозначения

Отсутствуют.

6 Обзор NB-IoT

Текущие тенденции развития технологий подвижной электросвязи приводят к изменению ее характера – на смену связи человека с человеком приходит связь человека с вещью и даже вещи с вещью. Закономерным результатом такой эволюции становится интернет вещей (IoT).

В сравнении с технологиями ближней связи, такими, например, как Bluetooth, ZigBee и др., сети сотовой связи характеризуются обширным покрытием, мобильностью и возможностью установки большого числа соединений, обеспечивая большее разнообразие сценариев применения, и станут основной технологией присоединения в IoT.

NB-IoT функционирует на базе сети сотовой подвижной связи, которая использует ширину полосы пропускания лишь порядка 180 кГц. Он может быть развернут непосредственно на основе сетей глобальной системы подвижной связи (GSM), универсальной системы подвижной электросвязи (UMTS) или на основе сетей на базе технологии долгосрочного развития (LTE) для снижения затрат и обеспечения бесшовного обновления.

Типичными характеристиками NB-IoT являются:

– низкий уровень рассеиваемой мощности – срок эксплуатации устройств NB-IoT может составлять от пяти до десяти лет;

– широкое покрытие в сравнении с сетью текущего стандарта в той же полосе частот NB-IoT дает выигрыш по мощности в 15–20 дБ и почти 100-кратное увеличение зоны покрытия;

– высокая пропускная способность – в одном секторе NB-IoT можно поддерживать порядка 100 000 устройств;

– низкая стоимость – одно устройство NB-IoT стоит около 5 долларов США.

Ожидается, что благодаря своему низкому уровню рассеиваемой мощности, широкому покрытию, низкой стоимости и высокой пропускной способности NB-IoT получит значительное распространение среди операторов и широкое применение в различных вертикальных отраслях.

7 Схема развертывания и типовые сценарии применения

7.1 Схема развертывания

7.1.1 Развертывание с использованием существующей базовой сети подвижной связи

В этом сценарии операторы развертывают NB-IoT, используя существующие базовые сети подвижной связи стандартов 2/3/4G.

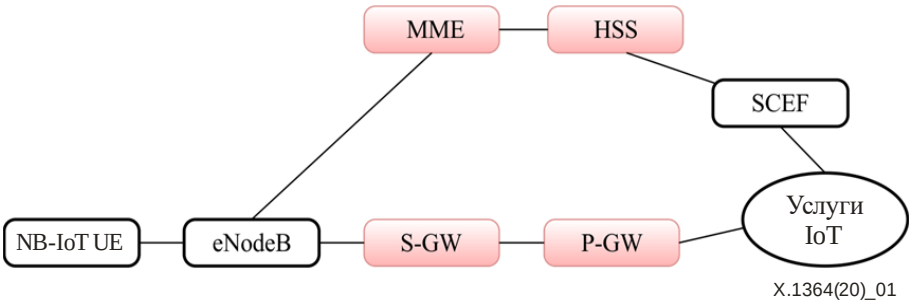
Такие элементы базовых сетей, как объект управления мобильностью (MME), обслуживающий шлюз (S-GW) и сетевой шлюз сети передачи данных с коммутацией пакетов (P-GW), необходимо оптимизировать для NB-IoT, чтобы обеспечить следующие характеристики [ETSI TS 123 401]:

– сверхнизкое энергопотребление оборудования пользователя (UE);

– большое число устройств в одной соте;

– применение узкополосных технологий радиодоступа (RAT), например сети расширенного универсального наземного радиодоступа (E-UTRA), сети универсального наземного радиодоступа (UTRA), GSM, CDMA2000; и

– расширенную зону покрытия.



ПРИМЕЧАНИЕ. – Элементы существующей базовой сети подвижной связи показаны розовым цветом.

Рисунок 1 – Развертывание с использованием существующей базовой сети подвижной связи

Помимо этих оптимизированных элементов на рисунке 1 представлены следующие элементы сети (см. [ETSI TS 123 401]):

– улучшенный узел B (eNodeB) – узел беспроводного доступа, на котором размещены функциональные элементы управления радиоресурсами, разуплотнения данных на линии вверх и шифрования потока пользовательских данных, маршрутизации данных плоскости пользователя и т. д.;

– сервер собственных абонентов (HSS), на котором хранится информация об абонентской подписке пользователей, например параметры аутентификации, информация о местоположении и т. п.;

– функция предоставления возможностей обслуживания (SCEF), которая обеспечивает безопасное предоставление услуг и возможностей сетевых интерфейсов 3GPP.

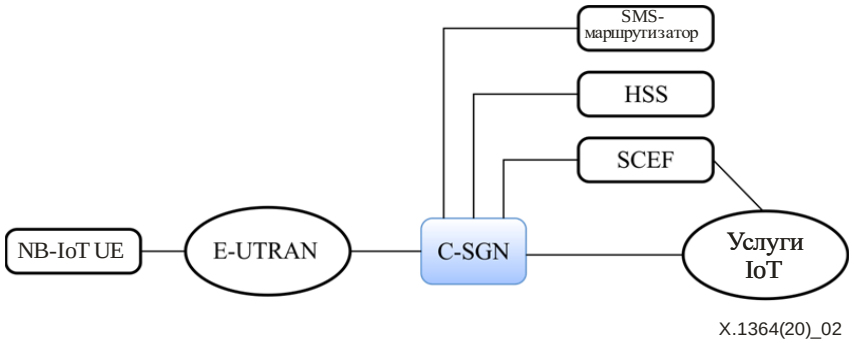
Эти элементы сети наряду со своими функциями обеспечивают поддержку предоставления услуг NB-IoT через сеть подвижной электросвязи.

7.1.2 Развертывание с использованием вновь созданной выделенной базовой сети подвижной связи

В этом сценарии развертывания операторы создают выделенную базовую сеть подвижной связи специально для предоставления услуг NB-IoT.

Узел обслуживающего шлюза (C-SGN) сотового интернета вещей (CIoT) определен в документе [ETSI TS 123 401].

C-SGN поддерживает подмножество и необходимую функциональность элементов базовой сети существующей улучшенной системы пакетной передачи данных (EPS). Он представляет собой совмещенный узел улучшенных базовых сетей пакетной передачи данных (EPC) и позволяет реализовать вариант развертывания с минимальным числом физических объектов EPS путем совместного размещения функций этих объектов в трактах плоскости управления и плоскости пользователя. C-SGN совмещает в себе функции MME, P-GW и S-GW, обеспечивая высокооптимизированное CIoT-решение. Реализация C-SGN поддерживает необязательные элементы функциональности своих внешних интерфейсов. Эти интерфейсы сопоставлены интерфейсам соответствующих объектов EPC – MME, S-GW и P-GW.



ПРИМЕЧАНИЕ. – Элементы вновь созданной базовой сети подвижной связи показаны голубым цветом.

Рисунок 2 – Развертывание с использованием вновь созданной выделенной базовой сети подвижной связи

Помимо этих элементов вновь созданной сети на рисунке 2 представлены следующие элементы сети (см. [ETSI TS 123 401]):

– сеть расширенного универсального наземного радиодоступа (E-UTRAN), функции которой включают сжатие заголовков и шифрование данных плоскости пользователя, выбор MME, принудительное задание скорости передачи данных на уровне носителя, контроль перегрузок, маркировку пакетов транспортного уровня на линии вверх и т. п.;

– сервер собственных абонентов (HSS), на котором хранится информация об абонентской подписке пользователей, например параметры аутентификации, информация о местоположении и т. п.;

– функция предоставления возможностей обслуживания (SCEF), которая обеспечивает безопасное предоставление услуг и возможностей сетевых интерфейсов 3GPP;

– маршрутизатор службы коротких сообщений (SMS), который обеспечивает передачу запроса на присоединение без попутного присоединения к EPS (запрос услуг EPS и сторонних услуг). Данная возможность доступна исключительно для оборудования пользователей, которое поддерживает только NB-IoT.

Эти элементы сети наряду со своими функциями обеспечивают поддержку предоставления услуг NB-IoT через сеть подвижной электросвязи.

7.2 Типовые применения

7.2.1 Дистанционное снятие показаний счетчиков

В этом сценарии применения устройство NB-IoT используется для снятия показаний приборов учета потребленных коммунальных услуг (например, воды, газа и т. п.) и дальнейшей передачи этих показаний по беспроводной сети поставщикам коммунальных услуг.

Применение технологии NB-IoT обеспечивает большее удобство, большую точность и эффективность снятия показаний по сравнению с традиционными ручными методами.

7.2.2 "Умная" стоянка автотранспорта

В этом сценарии применения устройства NB-IoT используются на парковке в качестве датчика наличия парковочных мест. Они дают водителям рекомендации по выбору парковочных мест и позволяют оплачивать парковку через интернет с помощью приложения для "умной" стоянки автотранспорта.

Применение технологии NB-IoT может облегчить поиск свободных парковочных мест и оплату парковки.

7.2.3 "Умное" сельское хозяйство

В этом сценарии применения устройства NB-IoT используются в качестве датчиков для регистрации параметров, имеющих значение в сельском хозяйстве: уровня засоленности, влажности, температуры и т. д. На основании этих данных сельскохозяйственные предприятия могут получать рекомендации по поливу и внесению удобрений.

Применение технологии NB-IoT способствует более рациональному ведению сельского хозяйства, поскольку позволяет анализировать информацию в режиме реального времени вместо проведения фермерами экспериментов традиционными методами.

8 Угрозы безопасности NB-IoT

Анализ угрозы безопасности NB-IoT имеет два важных аспекта – анализ с точки зрения характеристик и с точки зрения функциональной структуры уровней NB-IoT, как описывается в пунктах 8.1 и 8.2 соответственно.

8.1 Характеристики NB-IoT

Типичные характеристики NB-IoT – это низкий уровень рассеиваемой мощности, высокая пропускная способность, низкая стоимость и широкое покрытие.

8.1.1 Низкий уровень рассеиваемой мощности

1) Описание характеристики

К особенностям устройств NB-IoT относятся, в частности, низкое энергопотребление и долговечность, следствием чего являются менее частая потребность в подзарядке, низкая вычислительная мощность и т. д. Кроме того, встраиваемые системы отличаются сниженной ресурсоемкостью и большей простотой.

В основном системы, работающие на оконечном оборудовании традиционного IoT, характеризуются высокой вычислительной мощностью. В них применяются сложные сетевые протоколы передачи данных и строгие методы обеспечения безопасности. Ввиду повышенного энергопотребления они требуют частой подзарядки.

2) Угрозы безопасности NB-IoT

Угрозы отказа в обслуживании могут быть реализованы просто путем потребления всех ресурсов устройства NB-IoT. Стоимость осуществления таких атак на программное и аппаратное обеспечение относительно низка.

Учитывая такие особенности устройств NB-IoT, как сниженная ресурсоемкость, низкое энергопотребление и низкая вычислительная мощность, обеспечить шифрование данных при передаче в целях безопасности не представляется возможным. Иногда передача данных может вестись открытым текстом. Поэтому могут существовать значительные угрозы в плане аутентификации и проверки данных. Например, злоумышленники могут использовать несанкционированные устройства для установления связи с базовой станцией и передачи фальсифицированных данных.

8.1.2 Высокая пропускная способность

1) Описание характеристики

Пропускная способность NB-IoT гораздо выше, чем у традиционного IoT. Например, в одном секторе NB-IoT возможно подключение приблизительно 100 000 устройств.

2) Угрозы безопасности NB-IoT

При большом числе устройств даже незначительная уязвимость может критическим образом сказаться на безопасности сети. Например, троянская вирусная программа может заразить другое оконечное оборудование, в результате чего сеть станет недоступной.

В сценарии развертывания, в котором устройства NB-IoT могут использовать существующую базовую сеть подвижной связи, оконечное оборудование может заразить элементы этой сети (объект управления мобильностью, сервер собственных абонентов и другие устройства) с целью повлиять тем или иным образом на пользователей подвижной связи – например, отказать пользователям в доступе к сети или фальсифицировать абонентские данные для уклонения от оплаты телефонных звонков, SMS или трафика данных.

8.1.3 Низкая стоимость

1) Описание характеристики

Себестоимость устройств NB-IoT, как правило, весьма низкая.

2) Угрозы безопасности NB-IoT

Низкая стоимость устройств в числе прочего обеспечивается за счет применения упрощенных протоколов. Поэтому злоумышленники могут пользоваться уязвимостями этих протоколов и осуществлять атаки на устройства и сеть.

8.1.4 Широкое покрытие

1) Описание характеристики

Покрытие NB-IoT гораздо шире, чем у традиционного IoT. Например, по сравнению с сетями текущего стандарта NB-IoT дает выигрыш по мощности в 15–20 дБ в той же полосе частот, создавая зону покрытия, которая может быть в 100 раз больше.

2) Угрозы безопасности NB-IoT

Устройства, развернутые в удаленных точках, могут быть легко захвачены злоумышленниками и использованы для атак.

8.2 Уровни NB-IoT

8.2.1 Уровень устройства

Злоумышленники могут осуществлять атаки, копируя карты модуля идентификации абонента (SIM) в незаконных целях, таких как уклонение от оплаты доступа к сети.

Уязвимости могут существовать в стеках протоколов вновь разработанных облегченных оконечных модулей.

Производители существующего оконечного оборудования IoT при выводе на рынок нового оборудования с поддержкой NB-IoT могут брать за основу аппаратное обеспечение, поддерживающее Wi-Fi, Bluetooth, ZigBee и другие протоколы. Поскольку они могут попросту добавлять к этому оборудованию поддержку NB-IoT, в ходе разработки могут образовываться уязвимости и угрозы. Примерами могут служить ненадлежащая защита отладочных портов, применение нестойких алгоритмов шифрования, необновление аппаратного обеспечения и отсутствие своевременной проверки целостности данных, когда она необходима.

8.2.2 Сетевой уровень

Средства перехвата данных при передаче по сети позволяют вести мониторинг сеансов связи между оконечным оборудованием и базовыми станциями и перехватывать пакеты данных, которыми обмениваются эти компоненты. В таком случае злоумышленники могут анализировать уязвимости в системе безопасности на основе данных, извлеченных из перехваченных сообщений.

Учитывая большое число устройств и совместный доступ к сети подвижной электросвязи с ее абонентами, возможно наводнение сети сигнальным трафиком от поддельных устройств NB-IoT.

Не исключено также раскрытие данных из-за разнообразия видов данных, которые собираются службами NB-IoT, передаются по сети и обрабатываются многочисленными ее элементами.

Вследствие отсутствия механизма аутентификации между элементами сети сигнальный трафик в базовой сети NB-IoT может быть фальсифицирован, подделан или передан повторно.

Множество атак из интернета могут нарушить работу интерфейса между базовой сетью подвижной связи и интернетом. Например, в системе 5G это так называемый интерфейс N6 [ETSI TS 123 501]; этот интерфейс N6 соединяет функцию плоскости пользователя с интернетом.

8.2.3 Прикладной уровень

NB-IoT пригоден для применения в сценариях со статичным характером деятельности, малой чувствительностью к задержкам передачи, прерывистым перемещением и передачей данных в режиме реального времени.

Система, предназначенная для автоматического оповещения об аномалиях (например, датчик дыма) или периодического информирования (например, система мониторинга состояния окружающей среды), может не сработать или сработать ложно. Например, перехватив показания электросчетчика, установленного у того или иного пользователя, злоумышленник может подделать эти показания и лишить пользователя льгот.

В системах с дистанционным управлением (таких, как оборудование "умного" дома, которое может дистанционно включаться и выключаться пользователями) существует риск подачи злоумышленником вредоносных команд.

Системы NB-IoT тесно интегрированы с различными отраслями и как таковые подвержены уязвимостям, практически неизбежно возникающим в условиях использования сложной бизнес-логики и множества прикладных протоколов.

Возможный механизм злоупотребления услугами NB-IoT предусматривает, например, изъятие карты из штатного устройства при переустановке карты NB-IoT с оформленной абонентской подпиской из устройства NB-IoT в другое устройство или при рассылке SMS-спама с использованием этой карты и т. п.

9 Требования безопасности

9.1 Требования безопасности оконечных устройств

9.1.1 Физическая безопасность

В оконечном устройстве NB-IoT предусматривается физическая защита интерфейсов и микросхем, обеспечивающая невозможность для злоумышленника получить доступ к данным даже в случае кражи аппаратного обеспечения.

Для различных интерфейсов оконечное устройство NB-IoT поддерживает функции аутентификации и авторизации.

9.1.2 Безопасность обновлений

Требуется предусмотреть возможность обновления системы, программного обеспечения, аппаратного обеспечения и других элементов устройства NB-IoT для гарантирования безопасности системы и ее применений.

Во избежание злонамеренной подделки требуется обеспечить конфиденциальность и целостность файлов обновлений.

9.1.3 Защита конфиденциальности

Необходимо предусмотреть в оконечном устройстве NB-IoT гибкие механизмы защиты конфиденциальности для поддержки такой защиты в соответствии с требованиями к услугам NB-IoT.

9.2 Требования безопасности сети

9.2.1 Аутентификация

Для проверки подлинности объектов NB-IoT, использующих услугу NB-IoT, требуется обеспечить аутентификацию. Аутентификация позволяет гарантировать, что объект является именно тем, за который себя выдает, а не маскируется под штатный объект системы.

Учитывая характеристики NB-IoT, необходима облегченная аутентификация.

9.2.2 Предотвращение DDoS-атак

Для предотвращения атак на основе распределенного отказа в обслуживании (DDoS) и обеспечения своевременного реагирования на них требуется заблаговременно реализовать механизмы безопасности.

9.2.3 Безопасность сетевых объектов

Требуется предусмотреть возможности обеспечения безопасности в объектах базовой сети NB-IoT в целях предотвращения фальсификации данных, их злонамеренной подделки и атак с повторной передачей.

9.3 Требования безопасности приложений

9.3.1 Мониторинг соответствия требованиям к использованию/эксплуатации услуги

Требуется реализовать мониторинг соответствия требованиям к использованию/эксплуатации услуги для отслеживания пиковых значений, общего числа потоков и выявления аномалий в соответствии с требованиями к услугам NB-IoT.

9.3.2 Предотвращение злоупотребления услугами

Для предотвращения злоупотребления услугами, основанного на изъятии карты из штатного устройства, необходимо следить за характеристиками изменения международного идентификатора аппаратуры подвижной связи (IMEI).

9.3.3 Выявление, анализ и противодействие угрозам безопасности

Требуется обеспечить выявление, анализ и противодействие угрозам безопасности на основе анализа больших данных, описывающих поведение оконечных устройств NB-IoT.

10 Возможности обеспечения безопасности в NB-IoT

10.1 Возможности обеспечения безопасности в оконечном устройстве

В оконечном устройстве NB-IoT следует предусмотреть нижеперечисленные возможности обеспечения безопасности:

– SC_terminal device 1 – возможность управления ключами;
– SC_terminal device 2 – возможность согласования алгоритмов шифрования;
– SC_terminal device 3 – возможность шифрования данных;
– SC_terminal device 4 – возможность обеспечения целостности данных;
– SC_terminal device 5 – возможность безопасного обновления системы, программного обеспечения, аппаратного обеспечения и т. п.;
– SC_terminal device 6 – возможность реализации безопасных протоколов на базе облегченных алгоритмов шифрования.

10.2 Возможности обеспечения безопасности в сети

В сети NB-IoT следует предусмотреть нижеперечисленные возможности обеспечения безопасности:

– SC_network 1 – возможность управления ключами;
– SC_network 2 – возможность согласования алгоритмов шифрования;
– SC_network 3 – возможность шифрования данных;
– SC_network 4 – возможность обеспечения целостности данных;
– SC_network 5 – возможность контроля доступа (для исключения доступа несанкционированных объектов к элементам сети NB-IoT, хранимой информации, информационным потокам, услугам и приложениям);
– SC_network 6 – возможность обнаружения и/или предотвращения злонамеренных подделок;
– SC_network 7 – возможность защиты от DDoS-атак;

– SC_network 8 – возможность безопасной настройки;

– SC_network 9 – возможность выявления изъятия карты из штатного устройства.

10.3 Возможности обеспечения безопасности в приложениях

В приложениях NB-IoT следует предусмотреть нижеперечисленные возможности обеспечения безопасности:

– SC_applications 1 – защита от заражения вредоносным программным обеспечением с помощью антивредоносного программного обеспечения;

– SC_applications 2 – возможность мониторинга соответствия требованиям к использованию/эксплуатации услуги по ключевым показателям сети (например, пиковое значение, общее число потоков);

– SC_applications 3 – возможность обеспечения безопасности на уровне приложений для предотвращения угроз на основе анализа больших данных, описывающих поведение оконечных устройств NB-IoT.

10.4 Соотношение между возможностями обеспечения безопасности и требованиями безопасности

Возможности обеспечения безопасности, перечисленные в разделе 10, используются для удовлетворения некоторых требований безопасности, изложенных в разделе 9. Соотношение между возможностями обеспечения безопасности и требованиями безопасности показано в таблице 1.

Символ √ в ячейке таблицы 1 означает, что данное требование безопасности связано с конкретной возможностью обеспечения безопасности или, говоря точнее, обозначенное этим символом требование безопасности следует удовлетворять путем реализации указанной возможности обеспечения безопасности.

Таблица 1 – Соотношение между возможностями обеспечения безопасности и требованиями безопасности

Требования / Возможности	Физическая безопасность	Безопасность обновлений	Защита конфиденциальности	Аутентификация	Предотвращение DDoS-атак	Мониторинг соответствия требованиям к использованию/эксплуатации услуги	Предотвращение злоупотребления услугами	Выявление, анализ и противодействие угрозам безопасности
SC_terminal device 1	√			√				
SC_terminal device 2	√							
SC_terminal device 3			√					
SC_terminal device 4		√						
SC_terminal device 5	√	√						
SC_terminal device 6			√	√				
SC_network 1				√				
SC_network 2		√	√					
SC_network 3		√	√					
SC_network 4		√						
SC_network 5			√	√				
SC_network 6						√		
SC_network 7					√			
SC_network 8		√						
SC_network 9							√	
SC_applications 1		√						
SC_applications 2					√	√	√	
SC_applications 3			√					√

Библиография

[b-ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network.*

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

[b-ITU-T X.1141] Рекомендация МСЭ-Т X.1141 (2006 год), *Язык разметки, предусматривающий защиту данных (SAML 2.0)*.

[b-ITU-T X.1145] Recommendation ITU-T X.1145 (2017), *Security framework and requirements for open capabilities of telecommunication services*.

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

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, 2020 год