Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1813

(09/2022)

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

Безопасность сетей IMT-2020

Требования к безопасности и мониторингу для функционирования вертикальных услуг, поддерживающих сверхнадежную передачу данных с малой задержкой (URLLC), в частных сетях IMT-2020

Рекомендация МСЭ-Т X.1813

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 (1)	X.1140–X.1149
Безопасность приложений (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.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
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
Киберзащита	X.1590–X.1599
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
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	**X.1800–X.1819**

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

Рекомендация МСЭ-Т X.1813

Требования к безопасности и мониторингу для функционирования вертикальных услуг, поддерживающих сверхнадежную передачу данных с малой задержкой (URLLC), в частных сетях IMT-2020

Резюме

В Рекомендации МСЭ-Т X.1813 определены требования безопасности для функционирования вертикальных услуг, поддерживающих сверхнадежную передачу данных с малой задержкой (URLLC), в частной сети IMT-2020. Определены угрозы и риски, возникающие при предоставлении вертикальных услуг, поддерживающих URLLC, в частной сети IMT-2020, и описаны сценарии развертывания функций безопасности частной сети IMT-2020 для функционирования вертикальных услуг, поддерживающих URLLC. Мониторинг передаваемого контента не входит в сферу применения настоящей Рекомендации.

Частная сеть IMT-2020, называемая также закрытой сетью IMT-2020 (NPN), предназначена для исключительного использования частным объединением, например предприятием, и может быть развернута в различных конфигурациях с использованием как виртуальных, так и физических элементов. Она обеспечит надлежащую скорость, малую задержку и другие присущие IMT-2020 преимущества для поддержки приложений следующего поколения.

В вертикальных услугах умного предприятия и умных городов, использующих частную сеть IMT-2020, большое количество устройств интернета вещей (IoT) работают в режиме интенсивного межмашинного обмена (mMTC) и сверхнадежной передачи данных с малой задержкой (URLLC). Такая связь может быть подвержена угрозам безопасности и сопряженным с ними рискам. Кроме того, эти угрозы могут снизить устойчивость функционирования вертикальных услуг, поддерживающих URLLC. Сверхнадежная передача данных с малой задержкой не может быть гарантирована в условиях, когда качество работы вертикальных услуг ухудшается вследствие таких рисков.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1813	02.09.2022 г.	17-я	11.1002/1000/14991

Ключевые слова

DPI, обнаружение угроз и реагирование на угрозы на конечных точках, MEC, NPN, сетевой мониторинг, производительность, частная сеть IMT-2020, безопасность, UPF.

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора 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 соответствующим базам МСЭ-Т, доступным на веб-сайте МСЭ-Т, по адресу http://www.itu.int/ITU-T/ipr/.

© ITU 2023

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

		Стр.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	1
	3.1 Термины, определенные в других документах	1
	3.2 Термины, определенные в настоящей Рекомендации	2
4	Сокращения и акронимы	2
5	Соглашения	3
6	Обзор	4
7	Угрозы для вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020	6
8	Риски для вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020	6
9	Сценарии развертывания функций безопасности для функционирования вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020	7
10	Требования к безопасности и мониторингу для функционирования вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020	10
	10.1 Безопасность в отношении NMSF	10
	10.2 Безопасность в отношении NMCF	11
Приложение A – Характеристики NMSF		13
Приложение B – Характеристики NMCF		15
Приложение C – Визуализация результатов мониторинга		16
Дополнение I – Сценарии использования частной сети IMT-2020 для реализации вертикальных услуг		18
Библиография		21

Рекомендация МСЭ-Т X.1813

Требования к безопасности и мониторингу для функционирования вертикальных услуг, поддерживающих сверхнадежную передачу данных с малой задержкой (URLLC), в частных сетях IMT-2020

1 Сфера применения

Настоящая Рекомендация устанавливает требования безопасности для функционирования вертикальных услуг, поддерживающих сверхнадежную передачу данных с малой задержкой (URLLC), в частных сетях IMT-2020. В ней определены угрозы и риски, возникающие при предоставлении вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020, и описаны сценарии развертывания функций безопасности частных сетей IMT-2020 для функционирования вертикальных услуг, поддерживающих URLLC.

По соображениям защиты конфиденциальности мониторинг содержания сообщений не входит в сферу применения настоящей Рекомендации.

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.

[ITU-T Y.3102] Recommendation ITU-T Y.3102 (2018), *Framework of the IMT-2020 network.*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 закрытая сеть 5G (5G non-public network) [b-3GPP TS 22.261]: Сеть 5G, предназначенная для частного использования.

3.1.2 атака (attack) [b-ISO 13491-1]: Попытка злоумышленника получить или изменить на устройстве конфиденциальную информацию или услугу, которую ему не разрешено получать или изменять.

ПРИМЕЧАНИЕ 1. – К сетевым функциям, в частности, относятся функциональные возможности узла сети, такие как управление сеансом, управление мобильностью и функции транспортировки, с определенными интерфейсами и функциональным поведением.

ПРИМЕЧАНИЕ 2. – Сетевые функции могут быть реализованы на специализированном оборудовании или в виде виртуализированных программных функций.

ПРИМЕЧАНИЕ 3. – Сетевые функции не считаются ресурсами; скорее любые сетевые функции могут быть реализованы с использованием ресурсов.

3.1.3 развертывание (deployment) [b-ISO/IEC/IEEE 24765]: Этап проекта, на котором система вводится в эксплуатацию и решаются проблемы переходного периода.

3.1.4 домен (domain) [b-ISO/IEC 14888-1]: Совокупность объектов, действующих в рамках единой политики безопасности.

ПРИМЕР: сертификаты открытых ключей, созданные одним центром сертификации или несколькими такими центрами, придерживающимися одной и той же политики безопасности.

3.1.5 интернет вещей (Internet of things (IoT)) [b-ITU-T Y.4000]: Глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.

3.1.6 сетевой мониторинг (network monitoring) [b-ISO/IEC 27033-1]: Процесс непрерывного наблюдения и проверки регистрируемых данных об активности и операциях в сети, включая журналы аудита и оповещения и связанный с этим анализ.

3.1.7 сетевая функция (network function) [b-ITU-T Y.3100]: В контексте IMT-2020 – функция обработки в сети.

3.1.8 система (system) [b-ISO/IEC 27000]: Приложения, услуги, информационно-технологические ресурсы или другие средства обработки информации.

3.1.9 заинтересованная сторона (stakeholder) [b-ISO/PAS 19450]: Физическое лицо, организация или группа лиц, которые заинтересованы в планируемой, разрабатываемой или развертываемой системе или могут быть затронуты такой системой.

3.1.10 доверие (trust) [b-ISO/IEC 25010]: Степень уверенности пользователя или другой заинтересованной стороны в том, что продукт или система будут выполнять свои функции так, как это предполагалось.

3.1.11 вертикальная услуга (vertical service) [b-5G-PPP]: С точки зрения бизнеса вертикальной называется услуга, ориентированная на конкретную отрасль или группу клиентов со специализированными потребностями (услуги в автомобильной сфере, индустрии развлечений, услуги электронного здравоохранения, Индустрия 4.0).

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 система связи IMT-2020 (IMT-2020 communication system): Система управления процессами связи в сети IMT-2020 для услуг IMT-2020.

ПРИМЕЧАНИЕ 1. – Под 5G в контексте МСЭ-Т подразумевается IMT-2020.

ПРИМЕЧАНИЕ 2. – Для целей настоящей Рекомендации термины "система связи IMT-2020" и "система IMT-2020" идентичны.

3.2.2 экосистема IMT-2020 (IMT-2020 ecosystem): Совокупность заинтересованных сторон, взаимодействующих для формирования устойчиво работающей системы IMT-2020.

ПРИМЕЧАНИЕ. – Этот термин относится к развитию технологии связи 5G, при котором сообщество, включающее заинтересованные стороны из отрасли и академических организаций, вкладывает свои продукты, технологии и опыт для обеспечения функциональных возможностей на разных уровнях стека значений 5G, например на уровне инфраструктуры, сети, платформы, услуг и приложений.

3.2.3 частная сеть IMT-2020 (IMT-2020 private network): Закрытая сеть 5G (см. пункт 3.1.1), в которой используются виртуальные и физические элементы системы связи IMT-2020 и которая предназначена исключительно для использования частной структурой, например предприятием.

3.2.4 услуга IMT-2020 (IMT-2020 service): Преимущество, предоставляемое экосистемой IMT-2020.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

5GC	5G Core	Базовая сеть 5G
AMF	Access and Mobility Management Function	Функция управления доступом и мобильностью
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
DPI	Deep Packet Inspection	Углубленная проверка пакетов
EC	Edge Computing	Периферийные вычисления

EDR	Endpoint Detection and Response	Обнаружение угроз и реагирование на угрозы на конечных точках
GTP	GPRS Tunnelling Protocol	Протокол туннелирования GPRS
IoT	Internet of Things	Интернет вещей
MEC	Multi-access Edge Computing	Периферийные вычисления с множественным доступом
MEC DP	MEC Data Plane	Плоскость данных MEC
mMTC	massive Machine Type Communications	Массовая межмашинная связь
NF	Network Function	Сетевая функция
NMCF	Network Monitoring Client Function	Клиентская функция сетевого мониторинга
NMF	Network Monitoring Function	Функция сетевого мониторинга
NMSF	Network Monitoring Server Function	Серверная функция сетевого мониторинга
NPN	Non-Public Network	Закрытая сеть
PLMN	Public Land Mobile Network	Сеть сухопутной подвижной связи общего пользования
RTT	Round Trip Time	Время прохождения сигнала в обоих направлениях
SBA	Service-Based Architecture	Архитектура на основе услуг
SMF	Session Management Function	Функция управления сеансом
UDM	Unified Data Management	Единое управление данными
UE	User Equipment	Оборудование пользователя
UID	User ID	Идентификатор пользователя
UPF	User Plane Function	Функция плоскости пользователя
URLLC	Ultra-Reliable and Low Latency Communication	Сверхнадежная передача данных с малой задержкой

5 Соглашения

В настоящей Рекомендации используются следующие условные обозначения.

Ключевые слова "**требуется, чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления соответствия это требование не является необходимым.

Ключевое слово "**запрещается**" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Ключевые слова "**может факультативно**" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Данный термин не подразумевает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и что функция может быть активирована по желанию оператора сети (поставщика услуг) дополнительно. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии спецификации.

6 Обзор

Архитектура системы IMT-2020 обеспечивает поддержку операторов сетей передачи данных и услуг на основе таких методов, как виртуализация сетевых функций и сети с программируемыми параметрами. В 3GPP [b-3GPP TS 23.501] определена архитектура на основе услуг (SBA), в которой функциональность плоскости управления и общие хранилища данных сети IMT-2020 реализуются посредством совокупности сетевых функций (NF), каждой из которых разрешен доступ к услугам остальных. Архитектура системы IMT-2020 показана на рисунке 1.

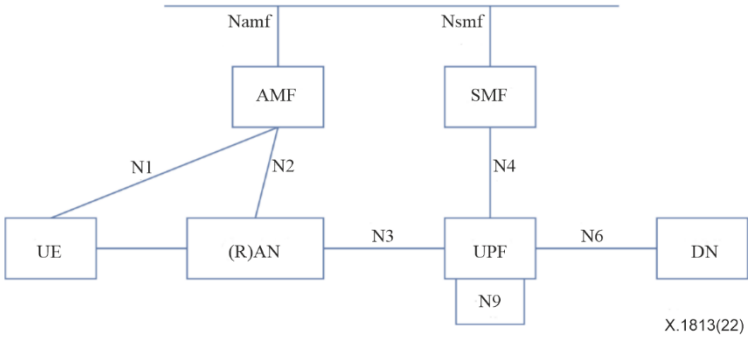

Рисунок 1 – Архитектура системы IMT-2020

Архитектура системы IMT-2020, определенная в [ITU-T Y.3102] и [b-3GPP TS 23.501], состоит из следующих сетевых функций:

– функция управления доступом и мобильностью (AMF), которая обеспечивает функции управления регистрацией, управления соединениями, управления мобильностью, функцию аутентификации доступа, функцию авторизации доступа, функцию управления услугами определения местоположения, функцию уведомления о событиях мобильности пользовательского оборудования (UE) и т. д.;

– сеть передачи данных (DN), например услуги оператора, доступ в интернет или сторонние услуги;

– функция управления сеансом (SMF), которая обеспечивает функции установления, изменения и освобождения сеанса, функции распределения IP-адресов оборудованию пользователя (UE) и управления ими, функцию выбора и управления плоскостью пользователя, сбор данных и поддержку интерфейсов тарификации, управление и координацию сбором данных тарификации в функции плоскости пользователя (UPF), уведомление о данных по линии вниз, поддержку сжатия заголовков и т. д.;

– функция плоскости пользователя (UPF) обеспечивает путь сеансов блоков данных протокола (PDU) в плоскости пользователя. 3GPP поддерживает развертывание с одной или несколькими UPF для данного сеанса PDU. Выбор UPF производит SMF. UPF обеспечивает распределение IP-адресов/префиксов оборудованию пользователя (UE) в ответ на запрос со стороны SMF, выполняет функцию маршрутизации и переадресации пакетов, проверку пакетов, QoS в плоскости пользователя, буферизацию пакетов на линии вниз, инициирование уведомления о данных по линии вниз и т. д.;

– Namf определяет интерфейс на основе услуг базовой функции управления доступом и мобильностью;

– Nsmf определяет интерфейс на основе услуг функции управления сеансом;

– UE – оборудование пользователя;

– (R)AN – сеть (радио)доступа.

В архитектуре системы IMT-2020 предусмотрены следующие эталонные точки:

– N1 – эталонная точка между UE и AMF;

– N2 – эталонная точка между (R)AN и AMF;

– N3 – эталонная точка между (R)AN и UPF;

– N4 – эталонная точка между SMF и UPF;

– N6 – эталонная точка между UPF и сетью передачи данных (DN);

– N9 – эталонная точка между двумя UPF.

Частные сети IMT-2020 предназначены для исключительного использования частным объединением, например предприятием, и могут быть развернуты в различных конфигурациях с использованием как виртуальных, так и физических элементов систем IMT-2020. Частная сеть IMT-2020 строится на принципах архитектуры системы IMT-2020, описанных в [b-3GPP TS 23.501], которые среди прочего включают гибкость и модульность во внедрении новой функциональности. Функциональная архитектура частных сетей IMT-2020 показана в Дополнении I.

Спецификациями 3GPP [b-3GPP TS 23.501] предусмотрены разнообразные сценарии развертывания частных сетей. На верхнем уровне частные сети IMT-2020 можно разделить на две категории:

– развертываемые в качестве полностью изолированных, автономных сетей;

– развертываемые как сегмент сети сухопутной подвижной связи общего пользования (PLMN) в связке с сетью общего пользования.

В то же время интернет вещей (IoT) определен в [b-ITU-T Y.4000] как глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий. В настоящей Рекомендации основной сценарий использования таких вертикальных услуг – это предоставление услуг IoT. В этом контексте устройства IoT могут представлять устройства оборудования пользователя, как определено 3GPP [b-3GPP TS 22.261].

В условиях, когда технология IMT-2020 перешла на стадию коммерческого внедрения, частные сети IMT-2020 будут использоваться главным образом для построения вертикальных услуг IMT-2020 на базе устройств IoT промышленного назначения – например, услуг для умных заводов и умных городов, которые требуют работы в режиме реального времени и сверхнадежной передачи данных с малой задержкой (URLLC). Поэтому частные сети IMT-2020 должны удовлетворять различным требованиям в отношении безопасности и производительности, поскольку они осуществляют обработку чувствительных ко времени доставки данных в соответствии с [ITU-T Y.3102]. На рисунке 2 показана общая архитектура безопасности частных сетей IMT-2020 согласно [b-3GPP TR 23.734].

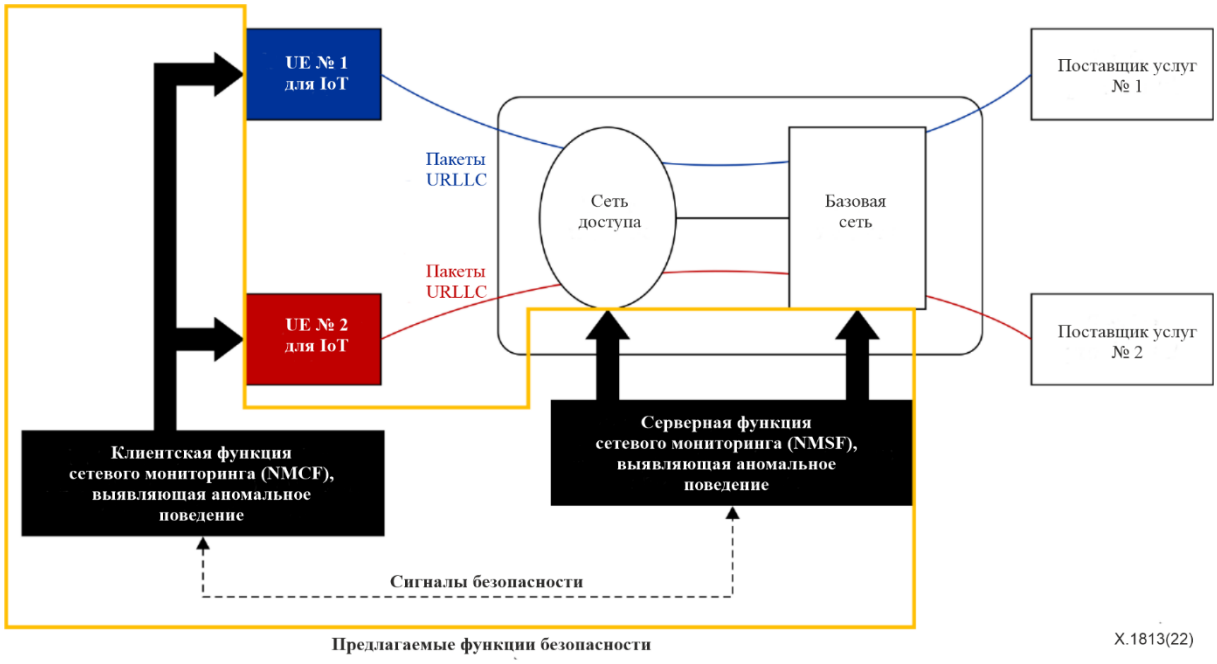

Рисунок 2 – Архитектура безопасности частных сетей IMT-2020

Как показано на рисунке 2, архитектура безопасности частных сетей IMT-2020 позволяет операторам вести мониторинг безопасности и производительности для связи между сетевыми узлами и оборудованием конечного пользователя в частной сети IMT-2020 для целей эксплуатации вертикальных услуг, поддерживающих URLLC.

7 Угрозы для вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020

IoT предоставляет широкий круг разнообразных новых интересных возможностей, таких как системы промышленной автоматизации и управления (IACS), связь между автономными транспортными средствами, умные электросети, датчики дорожного движения/трафика, связь беспилотных летательных аппаратов, медицинские датчики и средства дополненной и виртуальной реальности, работающие главным образом в автоматизированном режиме. Услуги IoT, возможно, должны соответствовать характеристикам URLLC для услуг в сетях IMT-2020. Согласно документу [b-3GPP TS 22.261] частные сети предназначены исключительно для использования частной структурой, такой как предприятие, и право на доступ к частной сети должно быть только у авторизованного оборудования пользователя.

В такой среде угрозами для вертикальных услуг являются среди прочего любые атаки, которые могут повредить работе компонентов и интерфейсов IMT-2020 в части задержек. Частная сеть IMT-2020 может развертываться с UPF или без таковой, а также с множественным доступом (MEC) или без такового. UPF доступна из интернета через интерфейс N6, определенный 3GPP. Поэтому если частная сеть IMT-2020 развернута с UPF и MEC, интерфейс N6 в значительной степени подвержен атакам, так как потенциальные злоумышленники имеют к нему доступ из любой точки интернета. Такие атаки могут умышленно или неумышленно совершаться как из-за пределов, так и изнутри частной сети IMT-2020.

Можно перечислить следующие виды угроз для UPF, MEC и интерфейса N6:

– атаки типа распределенный отказ в обслуживании (DDoS);

– прослушивание трафика (данных) на линиях связи;

– выработка неожиданно большого объема трафика или аномального трафика оборудованием пользователя в частной сети IMT-2020.

Частная сеть IMT-2020 развертывается частным образом и включает в себя сетевые компоненты и интерфейсы, часть из которых является новой и отличается с точки зрения безопасности от своих аналогов в составе традиционных сетей. В интерфейсе N3, который соединяет сеть доступа и базовую сеть, для защиты при транспортировании используется протокол IPsec. Интерфейс N4 соединяет UPF и AMF. Этот интерфейс закрыт в улучшенной базовой сети пакетной передачи данных (EPC) 4G, но не в vEPC IMT-2020. В отличие от X6, интерфейсы N3 и N4 недоступны из интернета, однако существует вероятность возникновения новых видов непреднамеренных угроз и препятствий.

Можно перечислить следующие виды угроз для интерфейсов N3 и N4:

– недостаточно эффективные методы управления доступом, реализованные в частной сети IMT-2020;

– ограниченность мер и процедур обеспечения безопасности, применяемых оператором частной сети IMT-2020;

– плохое проектирование или неправильная конфигурация сетевых компонентов частной сети IMT-2020, которые не учитывают внезапное увеличение масштабов доступа.

Отсутствие специалистов, освоивших многочисленные новые возможности сетей IMT-2020, может также сыграть роль непреднамеренной угрозы или препятствия.

8 Риски для вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020

По сути частная сеть IMT-2020 представляет собой сеть с высоким уровнем доверия в составе инфраструктуры IoT, так как она стандартизирована 3GPP для целей безопасной реализации новых вертикальных услуг IMT-2020.

Несмотря на применение традиционных методов обеспечения безопасности (аутентификации, авторизации и конфиденциальности данных), предусмотренных стандартами безопасности 3GPP, а также другими стандартами безопасности, частная сеть IMT-2020 может быть уязвимой к различным

рискам. Например, существующие методы обеспечения безопасности не могут нейтрализовать угрозы, связанные с аномальным поведением оборудования пользователя, размещенного в частной сети IMT-2020.

Поскольку характеристики сети IMT-2020 в большей степени ориентированы на программное обеспечение, они могут быть подвержены большему количеству рисков, связанных с недостатками в разработке ПО, неправильными процедурами обновления ПО, а также ошибками в конфигурации ПО. В результате возможно снижения производительности сети IMT-2020 из-за различных рисков, указанных выше.

В этом контексте последствия данных рисков могут включать:

– неустойчивое и опасное функционирование вертикальных услуг. Аномальное поведение устройств IoT, размещенных в сети IMT-2020, может вызвать угрозу для нормальной работы инфраструктуры умного города;

– уничтожение, модификация или изменение информации, хранимой или передаваемой в инфраструктуре сети IMT-2020;

– ухудшение показателей URLLC в сети IMT-2020: если сеть IMT-2020 не может гарантировать малую величину задержки в соответствии с требованиями URLLC, есть вероятность снижения производительности сети, что окажет негативное воздействие на соответствующие чувствительные ко времени вертикальные услуги. Например, поскольку умные заводы проектируются с учетом требований URLLC, возможно снижение качества и скорости выпуска продукции, если требования к короткой задержке не выполняются. Это может грозить не только громадными экономическими потерями, но и несчастными случаями на производстве. Другим примером может служить значительное ухудшение качества изображения с камер видеонаблюдения из-за задержек в передаче сигналов с различных датчиков.

Таким образом, для устранения вышеупомянутых угроз и рисков необходимо разработать требования безопасности для функционирования вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020.

9 Сценарии развертывания функций безопасности для функционирования вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020

В настоящем разделе изложены сценарии развертывания функций безопасности для функционирования вертикальных услуг, поддерживающих URLLC, в частной сети IMT-2020. Архитектура безопасности частной сети IMT-2020 конфигурируется посредством функций сетевого мониторинга (NMF). NMF состоит из серверной функции сетевого мониторинга (NMSF) и клиентской функции сетевого мониторинга (NMCF). NMF могут реализовываться функцией углубленной проверки пакетов (DPI), развернутой на узле сети, или выделенным узлом DPI.

NMSF могут быть сконфигурированы как независимые узлы сети, отделенные от UPF или MEC. В частности, NMSF соединяются с входом или выходом UPF или MEC для мониторинга соответствующих пакетов.

Есть три сценария развертывания NMSF:

A) NMSF как узел в составе MEC;

B) NMSF, реализованная как отдельный узел для мониторинга исходящего пакета от UPF;

C) множество NMSF, сконфигурированных так, чтобы первая функционировала как узел в составе MEC, а вторая – как отдельный узел для мониторинга исходящего пакета от UPF.

Во всех трех сценариях развертывания назначение или неназначение выделенных IP-адресов этим NMSF является вопросом реализации. Во всех этих сценариях NMCF встроена в оборудование пользователя.

На рисунке 3 показан сценарий развертывания A в архитектуре безопасности частной сети IMT-2020 с несколькими NMCF и NMSF.

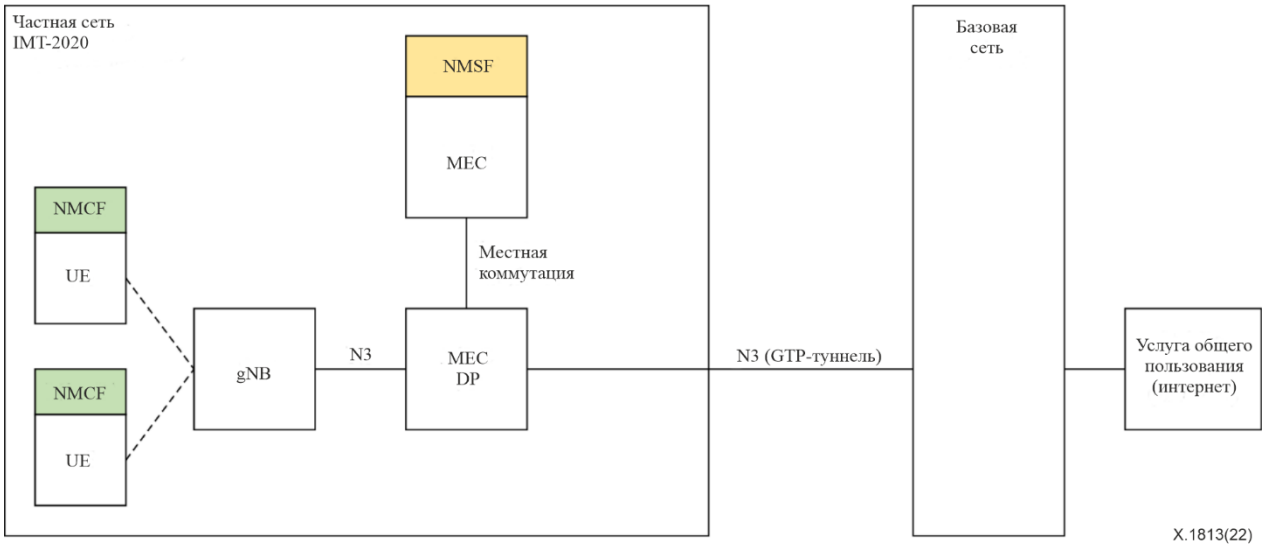

Рисунок 3 – Сценарий развертывания A

В ситуации, изображенной на рисунке 3, NMCF могут быть встроены в соответствующее UE, в частности в устройства IoT, осуществляющие связь с gNB. Размещение NMCF в устройствах IoT – одно из эффективных решений, обеспечивающих безопасность и соответствие требованиям URLLC в частной сети IMT-2020. NMCF могут реализовываться в программных обеспечениях и могут также обозначаться как объект обнаружения угроз и реагирования на угрозы на конечных точках (EDR) или микроядро (ME). Сервер NMCF может располагаться в частной сети IMT-2020, периферийном облаке или общедоступном сетевом домене (интернете). UE соединено с gNB беспроводной линией связи. Каждая единица UE передает пакеты в gNB или принимает пакеты от gNB. Узел gNB соединен с базовой сетью IMT-2020 или локальной сетью через интерфейсы N3 и N4. Пакеты проходят через эти интерфейсы.

Если NMSF назначен IP-адрес, NMCF и NMSF взаимодействуют друг с другом через интерфейсы N3 и N4 для обмена сигналами безопасности, например для передачи результатов мониторинга из NMCF.

Согласно сценарию A в плоскость данных MEC (MEC DP) может быть дополнительно встроена NMSF (не показана на рисунке 3), с тем чтобы две NMSF могли осуществлять мониторинг трафика частной сети и сети общего пользования в направлении UE и обратно. NMSF может быть также сконфигурирована как независимый и отдельный от MEC объект.

На рисунке 4 показан сценарий развертывания B в архитектуре безопасности частной сети IMT-2020 с несколькими NMCF и NMSF.

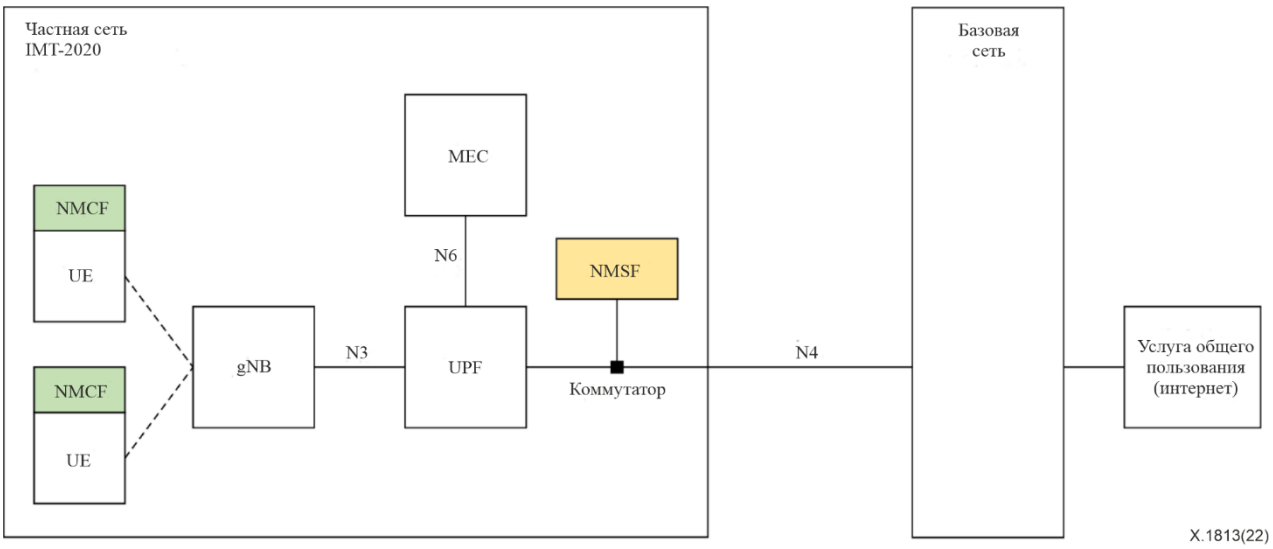

Рисунок 4 – Сценарий развертывания B

Как показано на рисунке 4, NMSF реализована как отдельный узел на выходе UPF, предназначенный для мониторинга исходящих пакетов от UPF. Для зеркального копирования пакетов от UPF может быть использован коммутатор. Если NMSF назначен IP-адрес, NMCF и NMSF взаимодействуют друг с другом через интерфейсы N3 и N4 для обмена сигналами безопасности, например для передачи результатов мониторинга с UE (клиентского узла). Если в частной сети IMT-2020 применяется межузловое шифрование (например, по протоколу IPSec), NMSF могут быть сконфигурированы в точке вывода расшифрованных пакетов из узла.

На рисунке 5 показан сценарий развертывания C в архитектуре безопасности частной сети IMT-2020 с несколькими NMF.

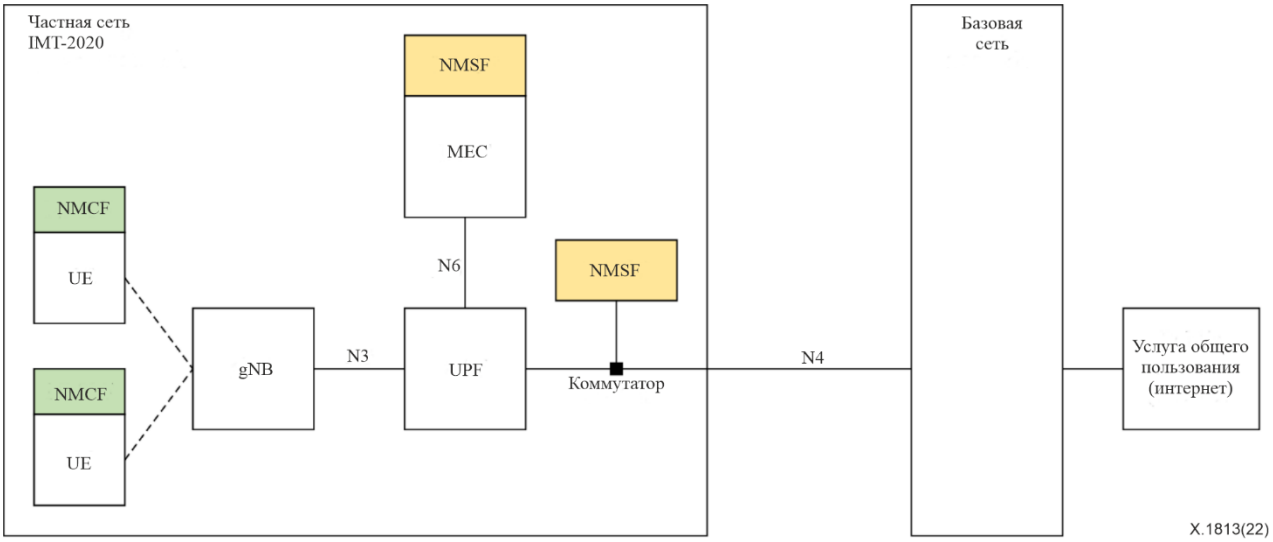

Рисунок 5 – Сценарий развертывания C

Как показано на рисунке 5, NMSF не только встроена в MEC, но и реализована как отдельный узел на выходе UPF, предназначенный для мониторинга исходящих пакетов от UPF. Если этим NMSF назначены IP-адреса, NMCF и NMSF взаимодействуют друг с другом через интерфейсы N3 и N4 для обмена сигналами безопасности, например для передачи результатов мониторинга с UE (клиентского узла). Если в частной сети IMT-2020 применяется межузловое шифрование (например, по протоколу IPsec), NMSF могут быть сконфигурированы в точке вывода расшифрованных пакетов из узла.

Приведенные выше три сценария не являются взаимоисключающими: выбор узла для использования зависит от затрат, характеристик сети и других факторов. Возможны также другие варианты развертывания NMSF и NMCF. Например, NMSF могут встраиваться в любой из узлов сети наряду с UPF и/или MEC.

Поэтому с точки зрения функциональной архитектуры сети мониторинг показателей безопасности и производительности может осуществляться путем использования NMSF, установленной в MEC, и/или UPF и NMCF, размещенных в устройствах IoT, и сигнального протокола между NMSF и NMCF.

10 Требования к безопасности и мониторингу для функционирования вертикальных услуг, поддерживающих URLLC, в частных сетях IMT-2020

В этом разделе определены требования к безопасности и мониторингу для функционирования вертикальных услуг, поддерживающих URLLC, в частной сети IMT-2020. Частная сеть IMT-2020 требует более высокого уровня защиты и эксплуатационных характеристик по сравнению с традиционными сетями ввиду большого объема данных, которыми обмениваются многочисленные клиентские устройства/датчики и управляющие ими центральные серверы. Кроме того, согласно [ITU-T Y.3102] требования URLLC IMT-2020 должны выполняться и на периферии (сети).

В сценариях развертывания частной сети IMT-2020 с NMCF и одной или несколькими NMSF общие требования к безопасности и мониторингу для функционирования вертикальных услуг, поддерживающих URLLC, включают следующее.

a) Требуется осуществлять мониторинг и обнаружение аномального поведения UE и частных сетей IMT-2020 в целях снижения рисков для безопасности.

b) Требуется осуществлять мониторинг показателей работы вертикальных услуг, поддерживающих URLLC.

c) Требуется оповещать администратора сети об аномальном поведении UE и частных сетей IMT-2020, с тем чтобы можно было решить проблемы и вовремя восстановить возможности URLLC в IMT-2020.

Рекомендуется также визуализировать аномальное поведение UE и частных сетях IMT-2020 для более эффективного его устранения. Визуализация результатов мониторинга описывается в Приложении C.

10.1 Безопасность в отношении NMSF

Безопасность в отношении NMSF включает следующее.

a) Требуется, чтобы NMSF обеспечивала по крайней мере функцию зеркального копирования пакетов, передаваемых между клиентским и серверным узлами, и создавала по крайней мере одну зеркальную копию пакета. Под клиентским узлом подразумевается UE или устройство IoT. Зеркальное копирование пакетов представляет собой метод сбора и анализа в реальном времени пакетов, обмен которыми производится на конкретном узле. Для зеркального копирования пакетов в NMSF может быть предусмотрена функция коммутации.

b) Требуется, чтобы на основании информации, содержащейся в зеркальных пакетах, NMSF выявляла аномальное поведение или нарушения в системе защиты, которые угрожают безопасности и производительности частной сети IMT-2020.

c) Если NMSF присваивается IP-адрес, требуется, чтобы NMSF получила от NMCF пакет проверки безопасности в формате TCP и вычислила время прохождения сигнала в обоих направлениях (RTT) по данным из этого пакета.

Структура пакета проверки безопасности в формате TCP показана на рисунке 6.

Заголовок TCP-пакета	Данные TCP (UID, результат мониторинга)

X.1813(22)

Рисунок 6 – Пакет проверки безопасности в формате TCP

Таблица 1 – Поля пакета проверки безопасности

Поле	Длина, байт	Описание
Идентификатор пользователя (UID)	4	Идентификатор пользователя, присвоенный UE
Длина	2	Длина в байтах поля результата мониторинга
Результат мониторинга	Переменная	Информация о работоспособности, загрузке центрального процессора и использовании памяти UE

d) Если NMSF не присваивается IP-адрес, требуется, чтобы NMSF создала зеркальную копию пакета проверки безопасности в формате протокола датаграм пользователя (UDP), переданного от NMCF на серверный узел, и вычислила время прохождения сигнала в обоих направлениях (RTT) по данным из зеркальной копии пакета проверки безопасности.

Структура пакета проверки безопасности в формате UDP показана на рисунке 7.

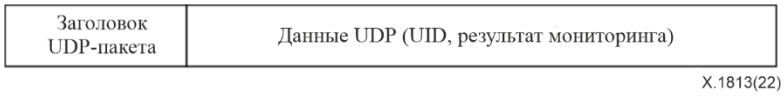

Рисунок 7 – Пакет проверки безопасности в формате UDP

Таблица 2 – Поля пакета проверки безопасности

Поле	Длина, байт	Описание
UID	4	Идентификатор пользователя, присвоенный UE
Длина	2	Длина в байтах поля результата мониторинга
Результат мониторинга	Переменная	Информация о работоспособности, загрузке центрального процессора и использовании памяти UE

e) Рекомендуется, чтобы NMSF оповещала об аномальном поведении, препятствующем выполнению требований URLLC, исходя из статуса безопасности и производительности. Обнаружив аномальное поведение, угрожающее безопасности и производительности, NMSF оповещает об этом пользователя, чтобы тот мог надлежащим образом отреагировать на это аномальное поведение. Затем NMSF передает оповещение на контроллер безопасности, тем самым предписывая контроллеру принять соответствующие меры в отношении аномального поведения, например остановить работу сети. Оповещение передается через интерфейсы N3 и N4, которые обеспечиваются протоколом сигнализации 3GPP.

Подробная реализация проводимого NMSF мониторинга безопасности и производительности методом зеркального копирования может осуществляться с использованием нормативного алгоритма из Приложения A.

10.2 Безопасность в отношении NMCF

Безопасность в отношении NMCF включают следующее.

a) Требуется, чтобы NMCF выполнялась на вычислительных ресурсах отдельных клиентских узлов или датчиков IoT. Рекомендуется, чтобы при этом использовалось минимальное количество ресурсов, обеспечивающее надлежащее выполнение функций.

b) Требуется, чтобы NMCF вела сбор пакетов или внутренней информации, передаваемой или принимаемой клиентскими узлами по сети.

c) Требуется, чтобы NMCF осуществляла мониторинг и обнаружение угроз сетевой безопасности, связанных с клиентскими узлами, включая саму NMCF, на основе данных из собранных пакетов или внутренней информации. Если значение того или иного параметра внутренней информации равно установленному пороговому значению или превышает его, NMCF определяет это как угрозу сетевой безопасности. Примерами внутренней информации являются загрузка центрального процессора клиентского узла, использование памяти клиентского узла и т. д.

d) Если NMSF присваивается IP-адрес, требуется, чтобы NMCF сгенерировала пакет проверки безопасности с использованием формата TCP, включая результат мониторинга, показанный на рисунке 6, и направила этот пакет в адрес NMSF.

e) Если NMSF не присваивается IP-адрес, требуется, чтобы NMCF сгенерировала пакет проверки безопасности в формате UDP, включая результат мониторинга, показанный на рисунке 7, и передала этот пакет на серверный узел для последующего зеркального копирования NMSF.

f) Рекомендуется, чтобы NMCF оповещала пользователя устройств IoT о любом случае аномального функционирования UE.

В случае NMCF больше вероятности собрать более точные данные. Вместе с тем работа NMCF может быть прекращена при возникновении тех или иных проблем, например при выключении питания нормально работающего оборудования. Поэтому мониторинг безопасности и производительности с использованием NMSF играет главную роль.

Однако мониторинг каждого потока данных от множества единиц UE, подключенных к частной сети IMT-2020, может стать чрезмерной нагрузкой для NMSF, поэтому для эффективного мониторинга угроз сети необходимо взаимодействие с NMCF.

Подробная реализация требований к NMCF может быть осуществлена с использованием нормативного алгоритма из Приложения B.

Приложение A

Характеристики NMSF

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Согласно настоящей Рекомендации NMSF выявляет аномальное поведение, угрожающее безопасности и производительности, на основе зеркально скопированных пакетов или связанной с ними информации. NMSF определяет частоту случаев аномального поведения, рассчитывая индексы или параметры, связанные с производительностью или безопасностью частной сети IMT-2020, и сравнивая результаты расчета с эталонными значениями в соответствии с требованиями к услугам связи (IMT-2020 или LTE). В данном случае эти требования могут быть известны из информации о доступе устройства IoT к сети интернета.

На рисунке A.1 показан метод измерения времени прохождения сигнала в обоих направлениях (RTT) с использованием зеркально скопированного пакета как показателя безопасности или производительности частной сети IMT-2020. По значению RTT можно выявлять аномальное поведение, угрожающее безопасности и производительности частной сети IMT-2020.

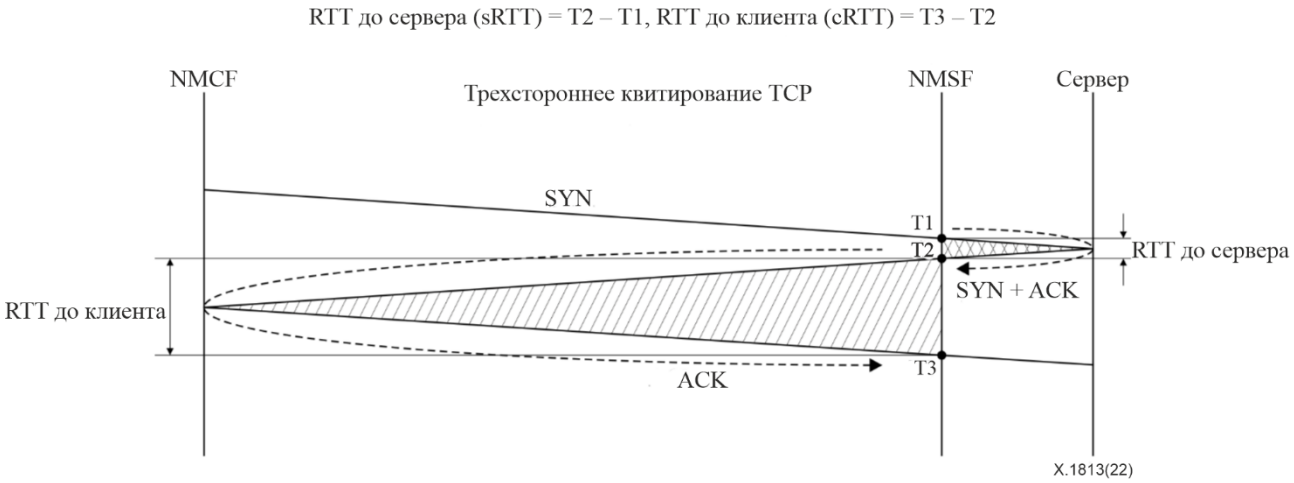

Рисунок A.1 – Измерение RTT

На рисунке A.1 изображен сценарий трехстороннего квитирования в отношении передачи и приема сигнала синхронизации (SYN), в котором NMSF вычисляет RTT сети, используя зеркальные копии пакетов, передаваемые по сети между пользователем и сервером. Например, после извлечения и сохранения меток времени приема и передачи трех пакетов (SYN, SYN + ACK и ACK), которыми обмениваются между собой NMCF (а именно клиент) и сервер NMSF (или MEC), NMSF гарантированно получает значение как минимум одного из временных параметров T1, T2 и T3. NMSF вычисляет RTT до сервера NMCF (sRTT) как T2 – T1, RTT до клиента (cRTT) – как T3 – T2, а общее RTT – как sRTT + cRTT или T3 – T1. Произведя такое вычисление для каждой транзакции, NMSF рассчитывает RTT для всей сети.

NMSF анализирует угрозы для безопасности или производительности частной сети IMT-2020, определяя, удовлетворяют ли sRTT, cRTT и RTT сети требованиям URLLC для частной сети IMT-2020. На рисунке A.2 показано, как выявлять участки снижения производительности по sRTT и cRTT в частной сети IMT-2020.

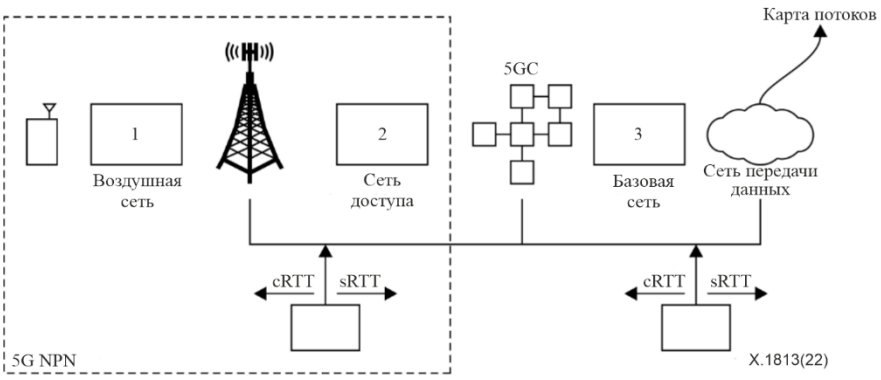

Рисунок A.2 – Выявление участков снижения производительности в частной сети IMT-2020

Помимо RTT, для выявления угроз для безопасности и производительности могут использоваться и другие индексы. Типичными примерами являются информация о времени ожидания отклика, то есть времени, за которое сервер NMSF (или MEC) получает первые данные, относящиеся к контенту по URL-адресу, связанному с клиентским запросом; информация о числе сеансов с ожиданием отклика, то есть количестве сеансов, еще не получивших отклика на клиентский запрос; BPS, CPS, TPS, ошибка HTTP 40x или 50x; информация о передаче и приеме данных, полученная из зеркально скопированного пакета; статистическая информация, полученная на выборке зеркально скопированных пакетов; информация о поддержании соединения, отражающая возможность подключения к устройству IoT или серверу NMCF.

Используя эти индексы, можно реализовать различными способами алгоритм выявления угроз для безопасности и производительности. Например, NMSF выявляет угрозу сетевой безопасности по информации о трафике (уровень 3 или 4 OSI), в том числе о прохождении пакетов и о протоколе (уровень 7 OSI).

Кроме всего перечисленного выше, могут применяться и другие методы обнаружения угроз безопасности, в том числе по данным пакетов (например, когда число соединений на участке сети между определенным исходным IP-адресом и конечным IP-адресом, BPS сервера или число запросов к URL-адресу превышает заданное пороговое значение, это рассматривается как угроза безопасности), по информации о трафике (например, превышение заданного порогового значения объема трафика по результатам кластеризации графа распределения трафика рассматривается как признак нарушения в системе безопасности частной сети IMT-2020), а также по данным протокола, аномалиям, сигнатурам, сведениям о нецелевом использовании, результатам анализа протоколов с сохранением состояния и спецификациям. Контент информации, передаваемой между NMCF и серверами NMCF, также может подвергаться контент-анализу со стороны NMSF.

Приложение B

Характеристики NMCF

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Для интеграции сервера NMCF и NMSF требуется протокол, который бы обеспечивал обмен информацией, относящейся к безопасности, между NMCF (или сервером NMCF) и NMSF.

Прежде всего NMCF определяет наличие угрозы для сетевой безопасности по состояниям устройств IoT, необходимых для его обслуживания, состоянию системы, данным журналов и значению RTT. Состояние устройства IoT, необходимого для обслуживания, включает в себя загрузку CPU, использование памяти и хранилища, а также информацию о поддержании соединения. Например, если использование памяти или показатель RTT превышают заданное пороговое значение, NMCF считает, что имело место аномальное поведение, угрожающее безопасности и производительности. Еще один пример – когда данные журналов указывают на попытку входа на клиентский узел с запрещенного IP-адреса или запуск неизвестного процесса. В этих случаях NMCF также определяет, что имело место аномальное поведение, угрожающее безопасности и производительности.

Далее NMCF передает определенное значение результата мониторинга наличия угрозы безопасности на сервер NMCF или в NMSF. Таким образом NMSF получает результат мониторинга угроз сетевой безопасности, воспринимаемой в конечной точке в режиме реального времени. На этом этапе следует идентифицировать устройство IoT по собранной сервером NMCF информации о NMCF и данным контент-анализа NMSF, чтобы можно было отличить контент, вырабатываемый конкретным устройством IoT, от контента других устройств.

Описанный выше метод позволяет снизить нагрузку на центральную NMSF за счет вынесения мониторинга угроз в конечные точки, такие как NMCF, и тем самым повысить эффективность мониторинга угроз безопасности и производительности сети.

Приложение C

Визуализация результатов мониторинга

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

На рисунке C.1 показан пример визуализации результатов мониторинга производительности сети (системы) и угроз безопасности с использованием NMSF.

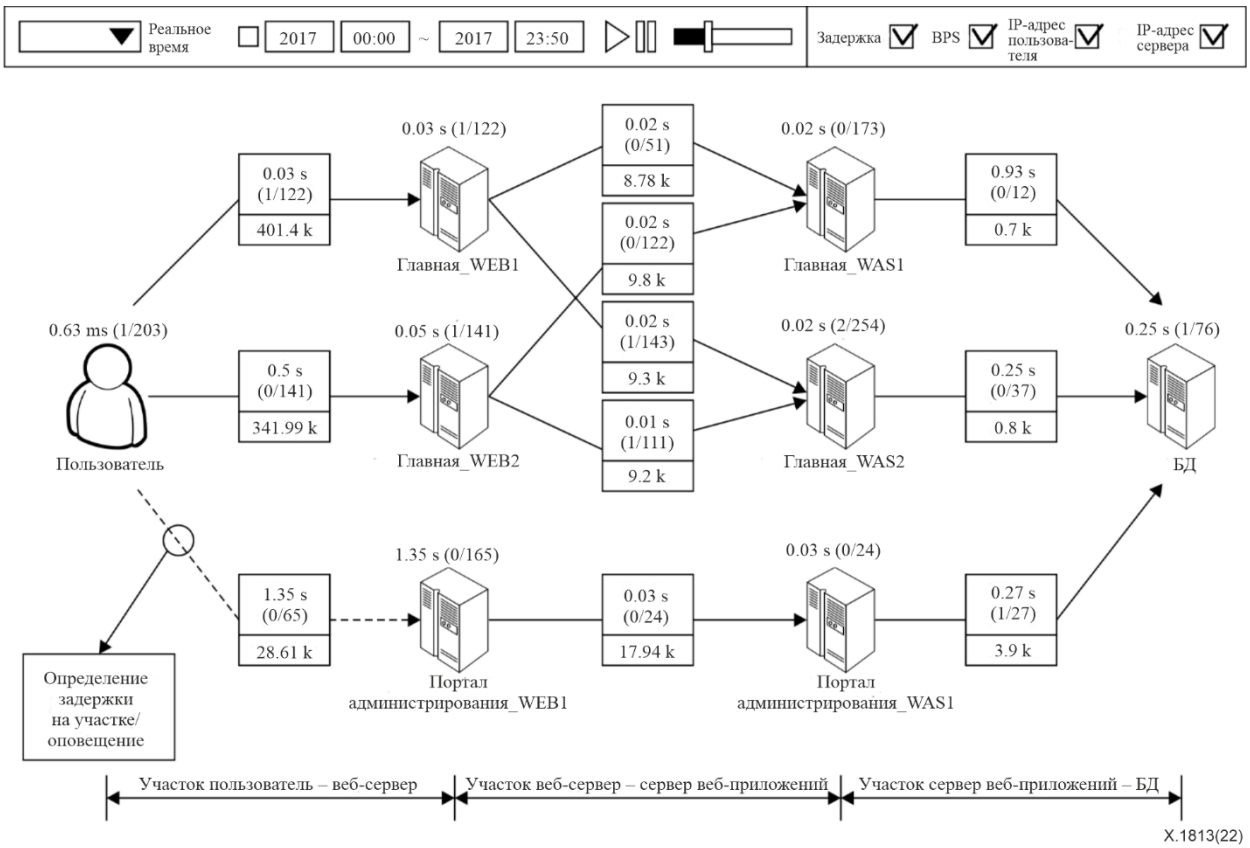

Рисунок C.1 – Пример визуализации результатов мониторинга производительности сети (системы) и угроз безопасности

Как представлено на рисунке C.1, результаты анализа показателей производительности или безопасности визуализируются в режиме реального времени и передаются в виде оповещений пользователям. Используя эти результаты, администраторы сетей могут незамедлительно устранить эти угрозы. Иными словами, результаты анализа интерпретируются с точки зрения производительности и безопасности сети, и при выявлении аномального поведения администраторы сети получают предупреждение.

Желательно, чтобы визуализация интуитивно понятно и четко отражала связи между объектами в сети. Визуализация реализуется следующим образом: NMSF генерирует объект, отражающий показатель безопасности и производительности, реализует этот объект в визуализируемом пространстве и строит карту потоков трафика в сети. Чтобы построить такую карту, генерируются объекты, отражающие показатели безопасности и производительности для первого и второго элементов, а затем для линии связи между этими элементами.

Для большей ясности линия между первым и вторым элементами отображается на карте потоков как объектное представление относящихся к ней показателей безопасности и производительности. Подчеркнуть различия можно, добавив элемент цвета. Иными словами, по крайней мере один из цветов, геометрических форм или толщин линий отчетливо визуализируется в соответствии со значениями показателей безопасности и производительности в сочетании с линиями связи.

С помощью функции визуализации можно обеспечить четкость и видимость на всех участках обслуживания. Она позволяет не только эффективнее предотвращать проблемы с сетевым обслуживанием, но и легко справляться с угрозами сети в рамках масштабной инфраструктуры IoT, например умных заводов и умных городов.

Дополнение I

Сценарии использования частной сети IMT-2020 для реализации вертикальных услуг

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В основе настоящей Рекомендации лежат три типа архитектуры частных сетей IMT-2020, показанные на рисунке I.1.

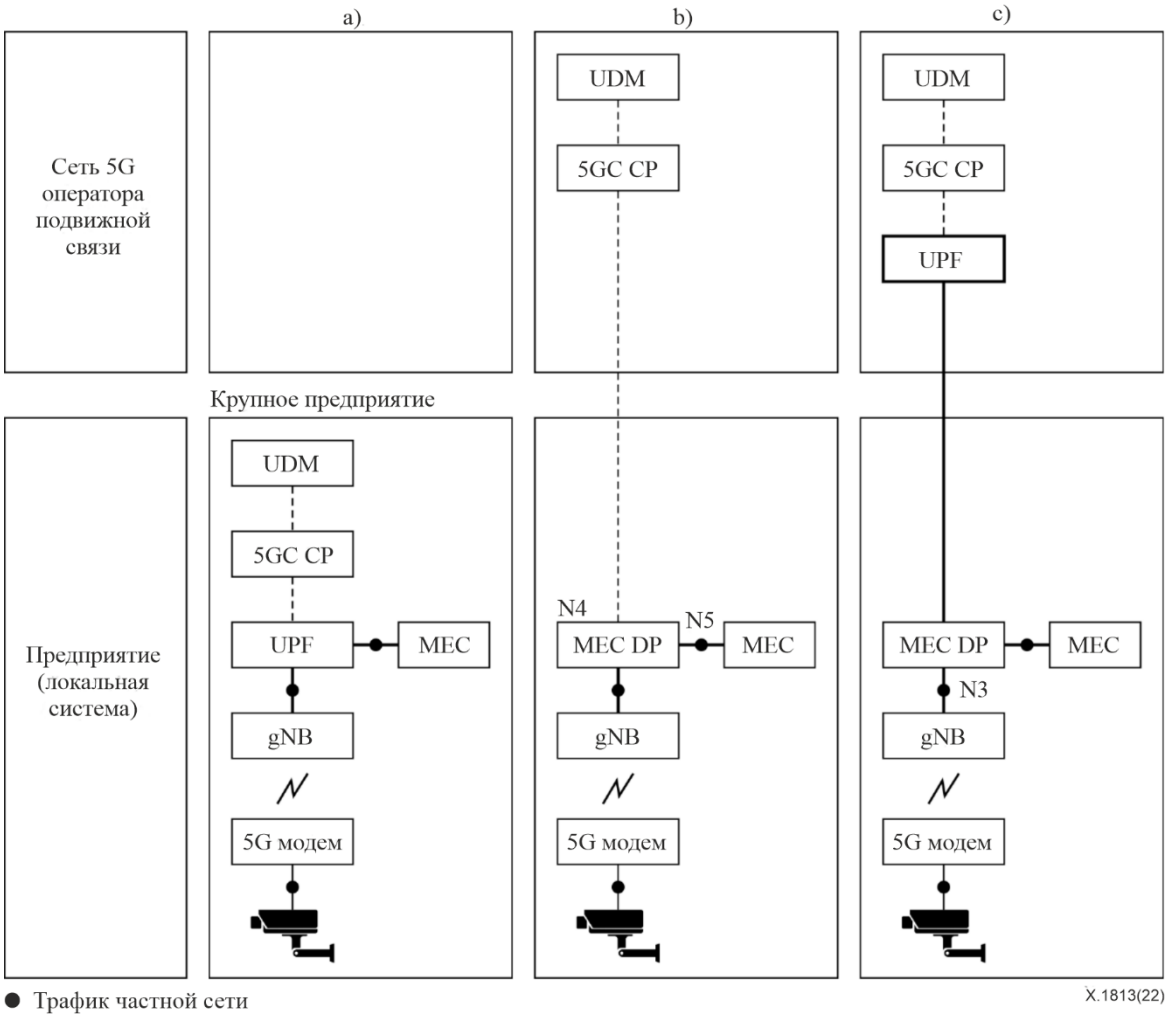

Рисунок I.1 – Три типа развертывания частных сетей IMT-2020

Согласно [b-Harrison] частная сеть IMT-2020 может развертываться как полностью изолированная, автономная сеть (a) или же как отрезок PLMN в связке с сетью общего пользования (b или c), как показано на рисунке I.1.

В варианте (a) частная сеть отделена от сети общего пользования физически, что обеспечивает полную безопасность данных. Поскольку сетевая задержка между устройством и сервером приложений находится в пределах нескольких миллисекунд, это позволяет реализовать прикладные услуги, поддерживающие URLLC.

Вариант (b) предполагает развертывание gNB, UPF и MEC внутри предприятия. В этой архитектуре RAN и плоскость управления являются общими для частных сетей и сетей общего пользования, и необходимо обеспечить повышенный уровень защиты и сократить задержку.

Вариант (c) предусматривает развертывание gNB, плоскости данных MEC (DP) и MEC внутри предприятия с размещением UPF в периферийном облаке оператора подвижной связи на удалении от устройств. Анализируя конечные IP-адреса пакетов всех GTP-туннелей, исходящих от gNB (декапсуляция GTP), MEC DP маршрутизирует IP-пакет пользователя во внутреннюю частную сеть, если он относится к локальному трафику. В такой архитектуре можно обеспечить повышенный уровень защиты и сократить задержку.

Согласно [b-Harrison] показанный на рисунке I.1 тип развертывания (b) может быть проиллюстрирован рисунком I.2 в вертикальном представлении с использованием нарезки сети. На рисунке I.2 показана подробная функциональная архитектура типа развертывания (b) с рисунка I.1, являющегося общим для частных сетей и сетей общего пользования IMT-2020.

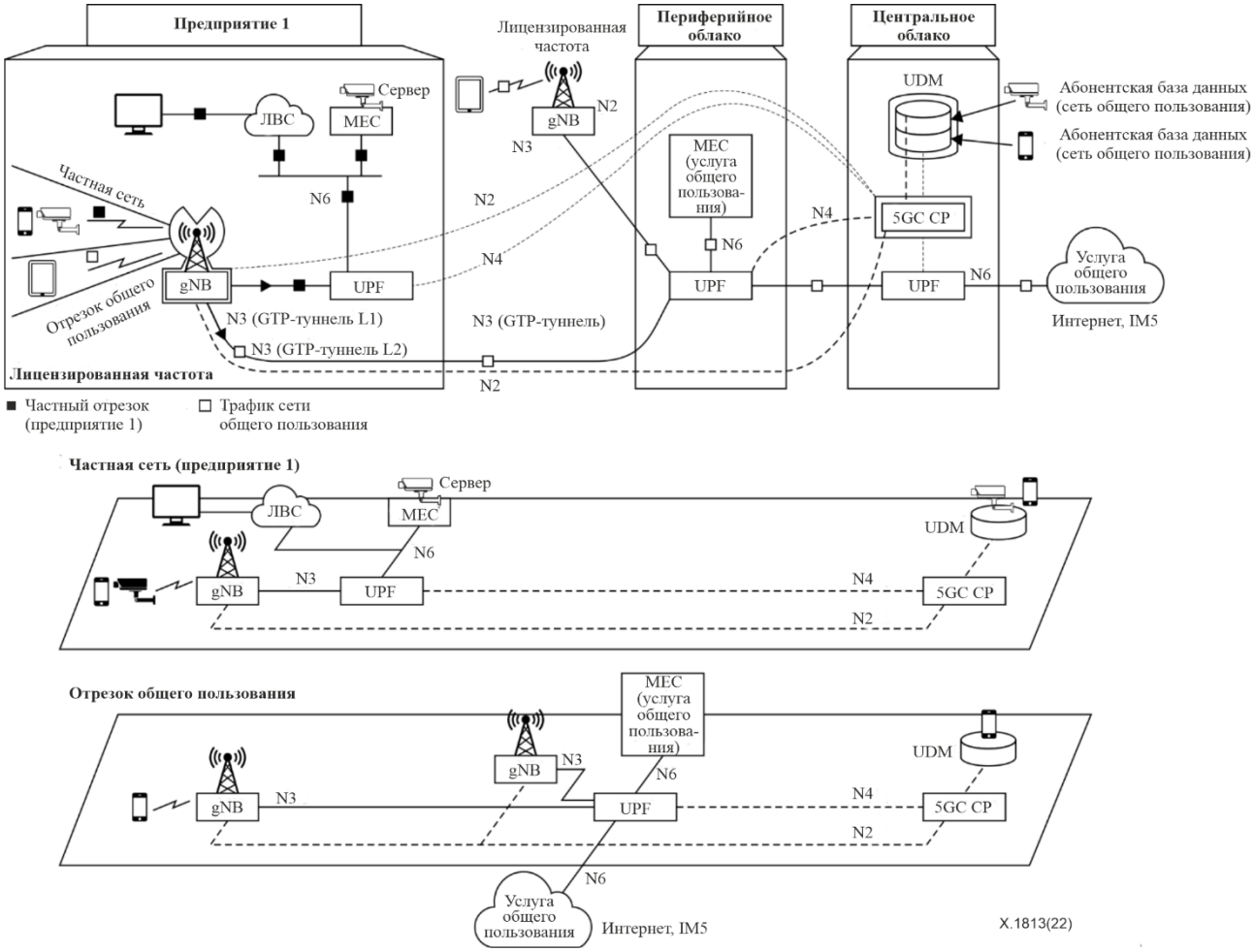

Рисунок I.2 – Подробная функциональная архитектура типа развертывания (b) с рисунка I.1

Согласно [b-Harrison] показанный на рисунке I.1 тип развертывания (c) может быть проиллюстрирован рисунком I.3 в вертикальном представлении с использованием нарезки сети. На рисунке I.3 показана подробная функциональная архитектура типа развертывания (c) с рисунка I.1, являющегося общим для частных сетей и сетей общего пользования IMT-2020.

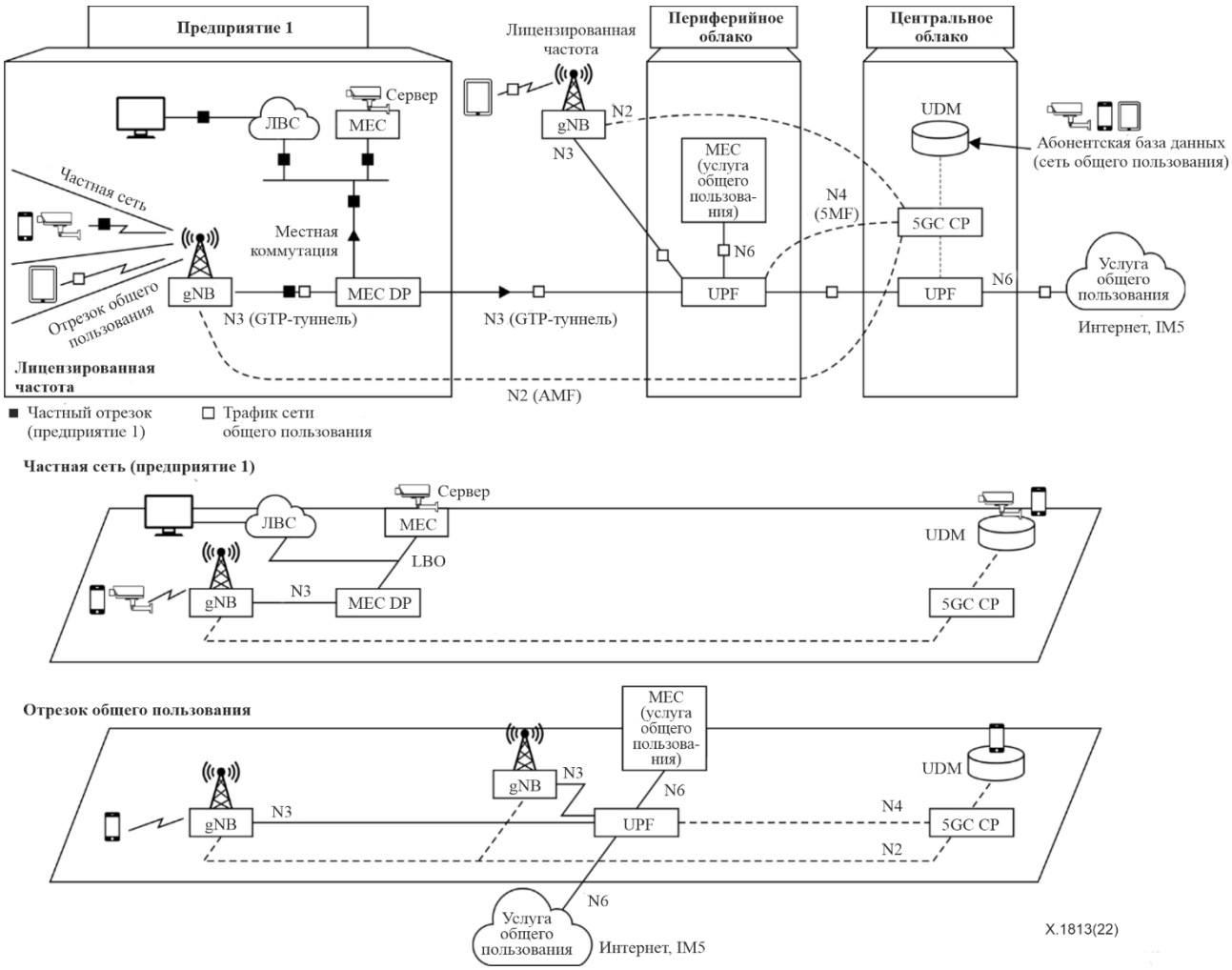

Рисунок I.3 – Подробная функциональная архитектура типа развертывания (c) с рисунка I.1

Все упомянутые выше типы функциональной архитектуры частной сети IMT-2020 развертываются операторами сетей в целях повышения безопасности и улучшения показателей URLLC. Поддержание надлежащей производительности и безопасности частной сети IMT-2020 является одним из важнейших факторов для вертикальных услуг, поддерживающих URLLC. Одним из возможных методов достижения этой цели является углубленная проверка пакетов (DPI), описанная также в [b-ITU-T Y.2774] и [b-ITU-T Y.2775]. Однако сфера применения этих Рекомендаций ограничена сетями подвижной связи общего назначения, и поэтому они неприменимы к частной сети IMT-2020 и, в частности, к вертикальным услугам, поддерживающим URLLC.

Библиография

[b-ITU-T Y.2774] Рекомендация МСЭ-Т Y.2774 (2019 г.), *Функциональные требования углубленной проверки пакетов в будущих сетях*.

[b-ITU-T Y.2775] Recommendation ITU-T Y.2775 (2019), *Functional architecture of deep packet inspection for future networks.*

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[b-ITU-T Y.4000] Рекомендация МСЭ-Т Y.4000/Y.2060 (2012 г.), *Обзор интернета вещей.*

[b-ISO 13491-1] ISO-13491-1:2016, *Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods*. <https://www.iso.org/standard/61137.html>

[b-ISO/IEC 14888-1] ISO/IEC 14888-1:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*. <https://www.iso.org/standard/44226.html>

[b-ISO/IEC/IEEE 24765] ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary*. <https://www.iso.org/standard/71952.html>

[b-ISO/IEC 25010] ISO/IEC 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*. <https://www.iso.org/standard/35733.html>

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. <https://www.iso.org/standard/66435.html>

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*. <https://www.iso.org/standard/63461.html>

[b-ISO/PAS 19450] ISO/PAS 19450:2015, *Automation systems and integration – Object-Process Methodology*. <https://www.iso.org/standard/62274.html>

[b-3GPP TS 22.261] 3GPP TS 22.261 v17.2.0 (2020), *Service requirements for the 5G system (Stage 1, Release 17).* <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107>

[b-3GPP TS 23.501] 3GPP TS 23.501 v17.0.0 (2021), *System architecture for the 5G System (5GS); Stage 2 (Release 17).* <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>

[b-3GPP TR 23.734] 3GPP TR 23.734 v16.2.0 (2019), *Study on enhancement of 5G System (5GS) for vertical and Local Area Network (LAN) services*. <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3487>

[b-5G-PPP] 5G PPP Architecture Working Group (2019), *View on 5G Architecture, Version 3.0*. <https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf>

[b-Harrison] Harrison J. Son, (2020), *Private 5G network strategies of Mobile operators and None-mobile operators*.
<https://www.netmanias.com/en/?m=view&id=reports&no=14585>

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, 2023 г.