ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

# МСЭ-Т X.1815 (03/2023)

СЕРИЯ X: Сети передачи данных, взаимосвязь открытых систем и безопасность

Безопасность сетей IMT-2020

# Руководящие указания по обеспечению безопасности и требования безопасности для услуг периферийных вычислений IMT-2020

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 | X.1000-X.1099 |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1) | X.1100-X.1199 |
| БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА | X.1200-X.1299 |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2) | X.1300-X.1499 |
| ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ | X.1500-X.1599 |
| БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ | X.1600-X.1699 |
| КВАНТОВАЯ СВЯЗЬ | X.1700-X.1729 |
| БЕЗОПАСНОСТЬ ДАННЫХ | X.1750-X.1799 |
| **БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020** | **X.1800-X.1819** |

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

# Рекомендация МСЭ-Т X.1815

## Руководящие указания по обеспечению безопасности и требования безопасности для услуг периферийных вычислений IMT-2020


**Резюме**

Сеть IMT-2020 позволит предоставлять различные услуги с использованием инфраструктуры сети и вычислительных ресурсов, в том числе услуги усовершенствованной подвижной широкополосной связи (eMBB), услуги на базе интенсивного межмашинного обмена (mMTC) и услуги на базе сверхнадежной передачи данных с малой задержкой (URLLC). В соответствии с ключевыми характеристиками и требованиями, определенными для сети IMT-2020, требуется, чтобы она обладала улучшенными характеристиками эффективности, степени персонализации, интеллектуальности, надежности и гибкости.

В целях поддержки типовых услуг в сети IMT-2020, особенно услуг eMBB и услуг на основе URLLC, одной из основных технологий для достижения требуемых ключевых показателей эффективности (KPI) сети IMT-2020 – особенно в связи с требованием короткой задержки и эффективного использования полосы пропускания – признаны периферийные вычисления.

Периферийные вычисления позволяют оператору и сторонним поставщикам услуг развертывать услуги вблизи пунктов доступа пользователей, тем самым обеспечивая высокоэффективное предоставление услуг за счет сокращения времени сквозной задержки и уменьшения нагрузки на транспортную сеть.

Чтобы обеспечить безопасные развертывание и эксплуатацию услуг периферийных вычислений, необходимо проанализировать угрозы безопасности и соответствующие требования по обеспечению безопасности услуг периферийных вычислений и установить общую структуру системы безопасности.

Цель настоящей Рекомендации – проанализировать схемы развертывания и типовые сценарии применения услуг периферийных вычислений, в ней определены угрозы безопасности и требования безопасности, характерные для услуг периферийных вычислений в сетях IMT-2020, и, таким образом, устанавливаются средства обеспечения безопасности, позволяющие операторам защитить свои приложения.



**Хронологическая справка** *

| Издание | Рекомендация | Утверждение | Исследовательская комиссия | Уникальный идентификатор |
|---|---|---|---|---|
| 1.0 | МСЭ-Т X.1815 | 03.03.2023 г. | 17-я | 11.1002/1000/15113 |

**Ключевые слова**

Услуги периферийных вычислений, сеть IMT-2020, руководящие указания по обеспечению безопасности.


* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL https://handle.itu.int/ после которого укажите уникальный идентификатор Рекомендации.

## 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 на программное обеспечение, 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.1815

# Руководящие указания по обеспечению безопасности и требования безопасности для услуг периферийных вычислений IMT-2020

## 1 Сфера применения

В настоящей Рекомендации приведена возможная схема развертывания и типовые сценарии применения услуг периферийных вычислений, определяются угрозы безопасности и требования, характерные для услуг периферийных вычислений в сетях IMT-2020, и, таким образом, представляются руководящие указания по средствам обеспечения безопасности, позволяющие операторам защитить свои приложения.

## 2 Справочные документы

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

[ITU-T Y3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network*.

[3GPP TS 23.501] 3GPP TS 23.50 (2022), *5G; System architecture for the 5G System (5GS) (version 17.4.0 Release 17)*.

## 3 Определения

### 3.1 Термины, определенные в других документах

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

**3.1.1 IMT-2020** [b-ITU-T Y.3100]: (Согласно [b-ITU-R M.2083]) Системы, компоненты систем и соответствующие технологии, которые обеспечивают гораздо более развитые возможности по сравнению с описанными в [b-ITU-R M.1645].

**3.1.2 троянский конь (троян) (Trojan horse)** [b-ITU-T E.800]: Программное обеспечение, которое представляется благоприятным или даже полезным. Оно скрывает свою реальную цель, направленную на разрушение системы или кражу информации.

### 3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

**3.2.1 услуги периферийных вычислений IMT-2020**: Услуги, предоставляемые через систему IMT-2020, которые могут располагаться рядом с пунктами доступа для пользовательского оборудования, тем самым обеспечивая эффективное предоставление услуг за счет сокращения времени сквозной задержки и уменьшения нагрузки на транспортную сеть.

**3.2.2 система IMT-2020**: Система 3GPP, состоящая из сети доступа (AN) IMT-2020, базовой сети IMT-2020 и пользовательского оборудования (UE).

## 4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

| | | | |
|---|---|---|---|
| AF | Application Function | | Функция приложения |
| AMF | Access and Mobility Management Function | | Функция управления доступом и мобильностью |
| AN | Access Network | | Сеть доступа |
| CDN | Content Delivery Network | | Сеть доставки контента |
| EASDF | Edge Application Server Discovery Function | | Функция обнаружения периферийного сервера приложений |
| DDoS | Distributed Denial of Service | | Распределенный отказ в обслуживании |
| DC | Data Centre | ЦОД | Центр обработки данных |
| DN | Data Network | | Сеть передачи данных |
| DNN | Data Network Name | | Имя сети передачи данных |
| DNS | Domain Name System | | Система доменных имен |
| eMBB | enhanced Mobile Broadband | | Усовершенствованная подвижная широкополосная связь |
| EHE | Edge Hosting Environment | | Среда периферийного хостинга |
| GW-C | Gateway-Control Plane | | Плоскость шлюз-контроллер |
| GW-U | Gateway-User Plane | | Плоскость шлюз-пользователь |
| IMS | Internet protocol Multimedia Subsystem | | Мультимедийная подсистема на основе протокола Интернет |
| IP | Internet Protocol | | Протокол Интернет |
| KPI | Key Performance Indicator | | Ключевой показатель эффективности |
| MEC | Mobile Edge Computing | | Мобильные периферийные вычисления |
| mMTC | massive Machine Type Communications | | Интенсивный межмашинный обмен |
| NAT | Network Address Translation | | Преобразование сетевых адресов |
| NEF | Network Exposure Function | | Функция представления сети |
| NB IoT | Narrow Band Internet of Things | | Узкополосный интернет вещей |
| NFVO | Network Functions Virtualization Orchestrator | | Оркестратор виртуализации сетевых функций |
| NRF | Network Repository Function | | Функция сетевого репозитория |
| VNFM | Virtualized Network Function Manager | | Диспетчер виртуализированных сетевых функций |
| OSS | Operation Support Systems | | Системы эксплуатационной поддержки |
| PDU | Protocol Data Unit | | Блок данных протокола |
| PSA | Protocol data unit Session Anchor | | Опорная точка сеанса блока данных протокола |
| QoS | Quality of Service | | Качество обслуживания |
| RAN | Radio Access Network | | Сеть радиодоступа |

| | | |
|---|---|---|
| SBA | Service Based Architecture | Архитектура на основе услуг |
| SIM | Subscriber Identification Module | Модуль идентификации абонента |
| SMF | Session Management Function | Функция управления сеансом |
| TLS | Transport Layer Security | Безопасность транспортного уровня |
| UE | User Equipment | Оборудование пользователя |
| UPF | User Plane Function | Функция плоскости пользователя |
| URLLC | Ultra-Reliable Low Latency Communications | Сверхнадежная передача данных с малой задержкой |
| V2X | Vehicle to Everything | Связь транспортных средств с различными объектами |

## 5 Соглашения по терминологии

В настоящей Рекомендации:

ключевые слова "**требуется, чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящему документу;

ключевое слово "**следует**" означает требование, которое рекомендуется, но не является абсолютно необходимым. Для заявления о соответствии это требование не является обязательным.

## 6 Обзор технологии периферийных вычислений IMT-2020

Сеть IMT-2020 позволит предоставлять различные услуги с использованием инфраструктуры сети и вычислительных ресурсов, в том числе услуги усовершенствованной подвижной широкополосной связи (eMBB), услуги на базе интенсивного межмашинного обмена (mMTC) и услуги на базе сверхнадежной передачи данных с малой задержкой (URLLC) [ITU-T Y.3101]. В соответствии с ключевыми характеристиками и требованиями, определенными для сети IMT-2020, требуется, чтобы она обладала улучшенными характеристиками эффективности, степени персонализации, интеллектуальности, надежности и гибкости.

В целях поддержки типовых услуг в сети IMT-2020, особенно услуг eMBB и услуг на основе URLLC, одной из основных технологий для достижения требуемых ключевых показателей эффективности (KPI) сети IMT-2020 – особенно в связи с требованием короткой задержки и эффективности использования полосы пропускания – признаны периферийные вычисления.

Периферийные вычисления IMT-2020 позволяют оператору и сторонним поставщикам услуг развертывать услуги через систему IMT-2020 вблизи пунктов доступа пользователей, тем самым обеспечивая высокоэффективное предоставление услуг за счет сокращения времени сквозной задержки и нагрузки на транспортную сеть.

### 6.1 Схема развертывания

Имеется два возможных варианта архитектуры системы IMT-2020, описанной 3GPP в спецификации системы IMT-2020: с традиционным подходом к опорной точке и интерфейсу и с подходом, при котором функции базовой сети взаимодействуют друг с другом с использованием архитектуры на основе услуг (SBA).

На рисунке 6-1 показана архитектура системы IMT-2020, основанная на [3GPP TS 23.501].

С точки зрения оператора схема развертывания услуг периферийных вычислений IMT-2020 с использованием SBA может включать следующие сетевые функции IMT-2020:

– UPF (функция плоскости пользователя). UPF – это одна из сетевых функций (NF) базовой сети IMT-2020. Она отвечает за маршрутизацию и пересылку пакетов, проверку пакетов, управление качеством обслуживания (QoS) и внешним сеансом блока данных протокола (PDU) присоединенной сети передачи данных (DN) в архитектуре IMT-2020.

– AMF (функция управления доступом и мобильностью). AMF получает всю информацию, относящуюся к соединению и сеансу, от оборудования пользователя (UE) через интерфейс N1, а к сети (радио)доступа ((R)AN) – через интерфейс N2 (см. рисунок 1), но отвечает только за управление соединением и задачи обеспечения мобильности.

– SMF (функция управления сеансом). SMF – фундаментальный элемент SBA IMT-2020. Он в первую очередь отвечает за взаимодействие с отделенной плоскостью данных, создание, обновление и удаление сеансов PDU и управление контекстом сеансов с помощью UPF.

– EASDF (функция обнаружения периферийного сервера приложений). EASDF выполняет одну или несколько следующих функций: регистрация в сетевом репозитории (NRF) для обнаружения и выбора EASDF и обработка сообщений DNS в соответствии с инструкциями SMF. EASDF осуществляет прямую связь в плоскости пользователя (т. е. без какой-либо трансляции сетевых адресов (NAT)) с опорной точкой сеанса PDU (PSA) UPF через интерфейс N6 для передачи сигналов системы доменных имен (DNS), которыми они обмениваются с UE.

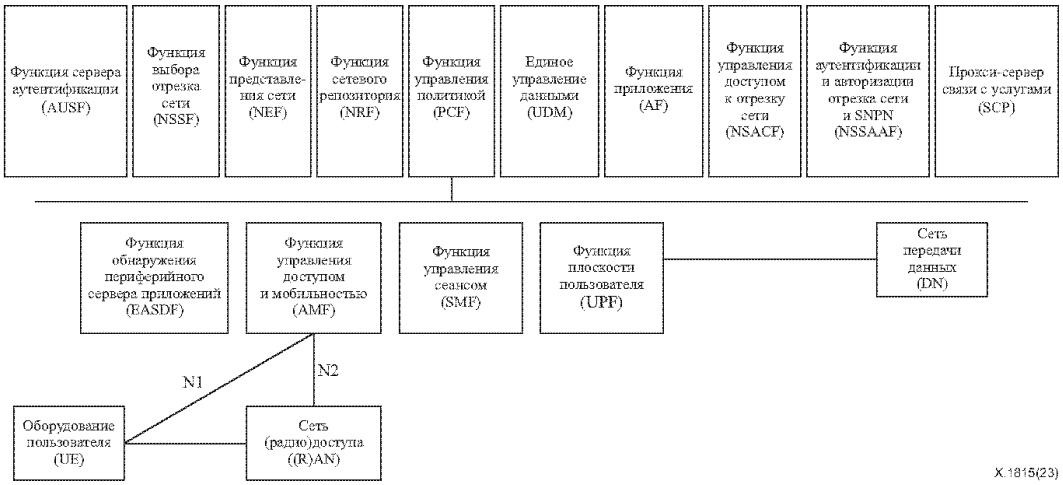


**Рисунок 6-1 − Архитектура системы IMT-2020**

На рисунке 6-2 показана схема развертывания услуг периферийных вычислений IMT-2020.

Система IMT-2020 поддерживает среду периферийного хостинга (EHE), развернутую в DN за пределами UPF PSA. Управление EHE могут осуществлять оператор или третьи лица [b-3GPP TS 23.548]. Локальная часть DN, в которой развернута EHE, может иметь соединение в плоскости пользователя как с централизованной PSA, так и с локальной PSA той же DNN.

Схема развертывания услуг периферийных вычислений IMT-2020, изображенная на рисунке 6-2, представлена с точки зрения оператора.

– Периферийный ЦОД. Предоставляет средства мобильных периферийных вычислений (MEC), которые позволяют использовать услуги периферийных вычислений IMT-2020, а также выполняет функции плоскости шлюз-пользователь (GW-U) и UPF.

– Локальный ЦОД. Выполняет функции GW-U, сети доставки контента (CDN) и UPF.

– Удаленный ЦОД. Выполняет функции плоскости шлюз-контроллер (GW-C), AMF/SMF, NB IoT, IMS и т. д.

– Домен управления. Включает в себя платформу управления облаком, оркестратора виртуализации сетевых функций (NFVO) и диспетчера виртуализированных сетевых функций (VNFM).

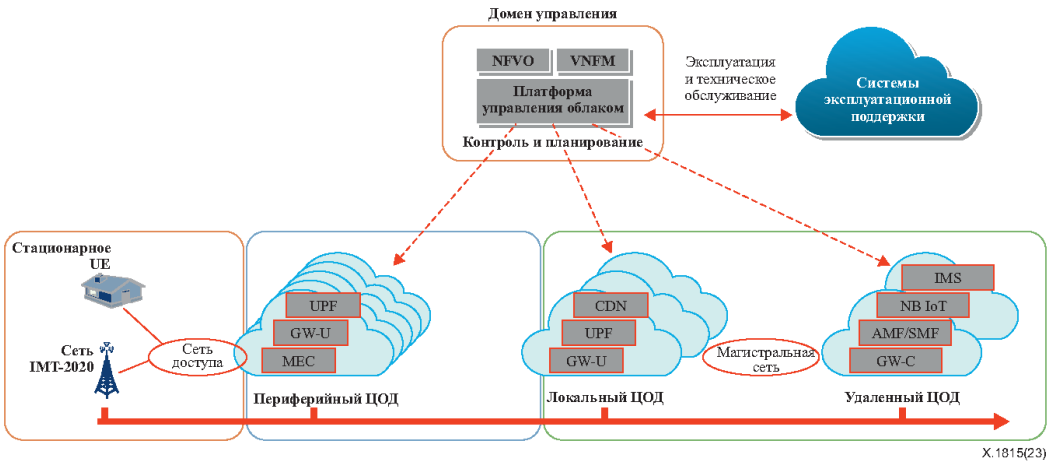


**Рисунок 6-2 – Схема развертывания услуг периферийных вычислений IMT-2020**

## 6.2 Типовой сценарий применения

### 6.2.1 Связь транспортных средств с различными объектами (V2X)

В сценарии V2X наличие большого количества подключенных устройств со множеством приложений приводит к повышению требований по передаче данных на стороне сети. Требуется, чтобы сеть обеспечивала расширенные возможности широкополосной передачи и обработки данных для их использования и хранения.

Благодаря применению в V2X технологии периферийных вычислений IMT-2020 становится возможным развертывание приложений в периферийных узлах, что уменьшает время сквозной задержки и повышает надежность в соответствии с конкретными требованиями различных услуг V2X (т. е. для услуги безопасного вождения необходимы строгие требования как к задержке, так и к надежности) за счет более короткого маршрута передачи и обеспечивает более мощные вычислительные ресурсы и ресурсы хранения.

В частности, могут предлагаться следующие услуги V2X на основе технологии периферийных вычислений IMT-2020.

– Услуги передачи информации. Услуги периферийных вычислений могут обеспечить функции загрузки и обновления карт, аудио- и видеоконтента, а также функции дистанционного обнаружения для транспортных средств. Для реализации этих функций требуется услуга периферийных вычислений с технологией усовершенствованной подвижной широкополосной связи, например, со скоростью передачи данных не менее 25 Мбит/с для услуг передачи видеоизображения высокого разрешения формата 4K.

– Услуги безопасного вождения. Услуги периферийных вычислений помогут водителю принимать решения по управлению транспортным средством (например, предупреждая о возможном столкновении) посредством сбора информации о транспортных средствах, пешеходах и придорожном оборудовании. Услуги периферийных вычислений должны обеспечивать возможности передачи данных с короткой задержкой и высокой надежностью (как правило, задержка должна составлять менее 20 мс, а надежность связи – не менее 99%).

– Услуги повышения эффективности вождения. Услуги периферийных вычислений оптимизируют эффективность систем управления дорожным движением на основе технологий V2X IMT-2020 и анализа больших данных, таких как системы управления светофорами или передачи указаний по скорости движения.

### 6.2.2 Интернет вещей (IoT)

Благодаря применению технологии периферийных вычислений IMT-2020 в сети IoT становится возможным развертывание приложений в периферийных узлах, чтобы сократить сквозную задержку за счет более короткого маршрута передачи и обеспечить более эффективное обслуживание за счет локальной обработки данных.

К сценариям услуг IoT на основе технологии периферийных вычислений IMT-2020 относятся, помимо прочего:

− "умный" город;

− "умное" здание;

− "умный" дом.

### 6.2.3 Промышленный интернет

Технология периферийных вычислений IMT-2020 поддерживает услуги промышленного интернета (особенно в случае приложений IoT реального времени, где обработка данных обычно происходит на удалении от централизованного центра обработки данных, а низкое значение задержки является обязательным требованием) путем координации сети IMT-2020 с периферийным контроллером, периферийным шлюзом и периферийным облаком.

Периферийный контроллер отвечает за координацию задач, развертывание приложений и управление жизненным циклом на уровне периферийного шлюза, а также управляет промышленными устройствами и т. д.

Периферийный шлюз выполняет координацию задач, регистрацию промышленных устройств, развертывание приложений и управление жизненным циклом на уровне периферийного облака, а также анализирует периферийные данные и т. д.

Периферийное облако отвечает за координацию задач, регистрацию промышленных устройств, развертывание приложений и управление жизненным циклом на уровне периферийного шлюза, а также координирует работу периферийных серверов, анализирует периферийные данные и т. д.

## 7 Угрозы безопасности

В рамках многоуровневой системы предложение услуги периферийных вычислений IMT-2020 охватывает уровень инфраструктуры, уровень сети и уровень приложений, поэтому необходимо рассматривать угрозы безопасности на всех этих уровнях. Важно отметить, что MEC обладает характеристикой безопасности и защиты конфиденциальности, поскольку передача данных происходит непосредственно на серверы MEC, а не через центральные серверы, что снижает риск утечки данных в процессе передачи данных в сети, однако эксплуатация большого количества мобильных устройств и развертывание периферийных облачных серверов приводит к новым проблемам безопасности. В частности, традиционные решения для обеспечения безопасности облачных вычислений могут не подходить для MEC, поскольку для среды устройств IoT на периферии возникает ряд новых угроз, которые существенно отличаются от возникающих при традиционном управлении облаком. На практике невозможно применить текущие методы защиты данных к периферийным устройствам, потому что большинство периферийных устройств ограничены в ресурсах, а сеть становится уязвимой из-за постоянно меняющейся среды MEC. Исчерпывающую оценку уязвимостей в MEC [b-ENISA] провело Агентство Европейского союза по кибербезопасности (ENISA), которое рассматривает спецификации 5G в соответствии с 3GPP версии 16. Таким образом, разработка среды MEC для будущих приложений 5G при обеспечении безопасности по-прежнему остается проблемой, требующей дальнейшего изучения в ближайшем будущем.

### 7.1 Уровень инфраструктуры

#### 7.1.1 Платформа управления облаком

Для развертывания услуг периферийных вычислений IMT-2020 может потребоваться платформа управления облаком. Помимо общих угроз безопасности для такой платформы, злоумышленник может использовать интерфейс между платформой управления облаком и сетью IMT-2020, чтобы впоследствии организовать атаку на сеть IMT-2020.

#### 7.1.2 Виртуализированная инфраструктура

Атака на физические ресурсы или их повреждение могут вывести из строя виртуализированную инфраструктуру. Злоумышленник может использовать эту потенциальную уязвимость системы для получения несанкционированного административного доступа к системе управления виртуальными ресурсами и изменения информации о конфигурации.

### 7.1.3 Внедрение вредоносных аппаратных/программных средств

В инфраструктуру могут быть несанкционированно внедрены программные или аппаратные компоненты, так называемые трояны, которые понижают эффективность работы периферийных серверов и устройств и даже позволяют эксплуатировать ресурсы поставщика услуг [b-Daniel]. Таким образом, организации, предоставляющие программные и аппаратные решения для услуг периферийных вычислений, могут оказаться невольными пособниками злоумышленников.

### 7.1.4 Физическое вмешательство в устройства

Физическое вмешательство в устройства становится более вероятным, поскольку в архитектуре периферийных вычислений вычислительные ресурсы расположены ближе к злоумышленникам. Злоумышленник может вывести из строя периферийные узлы, что в свою очередь поставит под угрозу эффективность работы всей сети.

## 7.2 Сетевой уровень

### 7.2.1 Анализ сетевых потоков

Злоумышленник может отслеживать и/или перехватывать данные в канале и анализировать характеристики потока, получая информацию об услугах и таким образом подготавливая дальнейшую атаку на сеть.

### 7.2.2 Выявление топологии сети

Злоумышленник может взломать узел предоставления услуг, установленный в незащищенной среде, и организовать атаку для выявления топологии сети.

### 7.2.3 DDoS-атака

Злоумышленник может взломать системы пользователей и/или узлы предоставления услуг, установленные в незащищенной среде, и организовать DDoS-атаку. При DDoS-атаке некоторый ресурс сети переполняется трафиком со стороны других, взломанных ресурсов, что приводит еще к одной угрозе безопасности периферийных вычислений.

### 7.2.4 Перехват передаваемых данных или манипулирование ими

Услуги, использующие периферийные вычисления IMT-2020, основаны на незащищенной беспроводной сети. Злоумышленник может перехватить передаваемые данные или манипулировать ими; в некоторых сценариях, например в промышленности и производстве или в "умном" городе, в передаваемых данных может содержаться чрезвычайно важная информация, такая как идентификаторы и учетные данные пользователей, деловые сведения и информация, относящаяся к общественной безопасности.

### 7.2.5 Междоменная атака

Услуга периферийных вычислений в сети IMT-2020 должна координировать функциональные возможности сети доступа, базовой сети и платформы управления облаком, поэтому это слабое звено может подвергнуться междоменной атаке, что приведет к неготовности сети и услуг.

### 7.2.6 Несанкционированный доступ

Для того чтобы UE могло подключаться к наилучшей услуге периферийных вычислений, UE и базовая сеть IMT-2020 должны обмениваться сигналами. Если злоумышленник вмешается в сигнализацию, он может получить несанкционированный доступ к услугам периферийных вычислений и даже организовать DDoS-атаку.

### 7.2.7 Представление сети периферийному приложению

Сеть IMT-2020 может предоставлять информацию о сети функциям локального приложения (AF). К возможным сценариям относятся UPF локальной PSA, предоставляющая информацию о сети локальной AF – непосредственно или через функцию представления локальной сети (NEF).

### 7.2.8 Атаки, связанные с информацией о маршрутах

Атака, связанная с информацией о маршрутах, или просто атака маршрутизации, осуществляется на сетевом уровне периферийной сети. Атаки маршрутизации нарушают порядок передачи трафика в сети, что может повлиять на пропускную способность, задержку и пути передачи данных.

### 7.2.9 Перехват сеанса

Злоумышленник перехватывает сеанс пользователя, чтобы получить доступ к его данным и услугам.

## 7.3 Уровень приложений

### 7.3.1 Уязвимость технической структуры

Поскольку в системе услуг периферийных вычислений IMT-2020 огромное количество узлов использует одну и ту же техническую структуру в разнообразных сценариях и вертикальных отраслях, взлом одного узла повлияет и на другие.

### 7.3.2 Несанкционированное использование

Угроза несанкционированного использования возникает, когда нелегитимный пользователь или пользователь, не оформивший подписку, получает доступ к услугам периферийных вычислений IMT-2020, маскируясь под авторизованный объект.

### 7.3.3 Трояны и вирусы

Атаки с использованием троянов и вирусов происходят, когда вредоносная услуга периферийных вычислений IMT-2020 или злоумышленник выдает себя за легитимного поставщика услуг и внедряет в приложение троян или вирус, способный причинить вред пользовательским устройствам и данным или даже запустить дальнейшую атаку на сеть подвижной связи.

### 7.3.4 Раскрытие данных

Раскрытие данных происходит, когда злоумышленник выдает себя за легитимный объект, чтобы в процессе переноса, передачи, хранения, совместного использования или уничтожения данных приложения, использующего услуги периферийных вычислений, извлечь эти данные.

# 8 Требования безопасности

## 8.1 Уровень инфраструктуры

Требования безопасности платформы управления облаком должны предусматривать:

a) чтобы платформа управления облаком поддерживала аутентификацию и авторизацию шлюза плоскости данных, управления платформой периферийных вычислений и приложения периферийных вычислений;

b) чтобы платформа защищала конфиденциальные данные, препятствуя несанкционированному доступу и подлогу данных (например, в промышленных сценариях необходимо защищать конфиденциальные технологические данные для корректного выполнения производственных процессов и предотвращения сбоев из-за сетевых атак);

c) чтобы платформа управления облаком была надежно изолирована с помощью элементов базовой сети IMT-2020 (например, NEF, UPF);

d) чтобы производился анализ побочного канала для обнаружения аппаратных троянов с использованием анализа времени выполнения операций, потребляемой мощности и температуры окружающего пространства. По сути, этот метод позволяет обнаруживать вредоносное микропрограммное или программное обеспечение, установленное на периферийных узлах, выявляя необычное поведение системы, такое как увеличение времени выполнения операций и энергопотребления;

e) чтобы для обнаружения вредоносных атак использовались методы обнаружения аппаратных троянов, когда пораженное трояном оборудование сравнивается с оборудованием, не пораженным трояном;

f) чтобы обеспечивалась физическая защита всех периферийных узлов, не находящихся в высокозащищенных периферийных центрах обработки данных, например дополнительные методы физической защиты на производстве или механизмы блокировки и другие средства физической защиты в полевых условиях;

g) наряду с вышеизложенным требуется, чтобы части периферийной системы, работающие с криптографическими материалами, были защищены от атак по побочному каналу, например с использованием защищенных, устойчивых SIM-карт.

Требования безопасности виртуализированной инфраструктуры должны предусматривать:

a) чтобы в случае если инфраструктура услуг периферийных вычислений IMT-2020 развернута на виртуальной машине, виртуальный ЦП, память и система ввода-вывода виртуальной машины были надежно изолированы;

b) чтобы виртуализированная инфраструктура поддерживала надежную изоляцию между контейнерами;

c) чтобы виртуализированная инфраструктура поддерживала зеркалирование репозиториев и подписей.

d) чтобы сегментация с нарезкой сети разделяла трафик и изолировала вычислительные ресурсы [b-ENISA].

### 8.2 Сетевой уровень

Требования безопасности системы передачи данных по сети должны предусматривать:

a) чтобы она поддерживала защиту конфиденциальности и целостности данных при их передаче;

b) чтобы в ней использовался протокол безопасности (например TLS v1.2) для создания безопасного канала связи между элементами сети;

c) использование шифрования трафика данных между сторонами с применением безопасного сквозного транспортного протокола, использование длинного случайного числа или строки в качестве ключа сеанса и создание нового идентификатора сеанса после каждого успешного входа в систему;

d) чтобы она поддерживала возможность защиты от DDoS-атак путем тщательной фильтрации трафика, так чтобы нелегитимные запросы не пропускались, а легитимные проходили без значительных задержек.

Требования безопасности системы управления сетью должны предусматривать:

a) чтобы система эксплуатационной поддержки (OSS) поддерживала аутентификацию и авторизацию при взаимодействии с платформой управления облаком;

b) чтобы обеспечивалась надежная изоляция функций между управлением услугами периферийных вычислений и OSS;

c) чтобы выполнялось постоянно отслеживание того, не работает ли сеть замедленно или неправильно, и производилось своевременное оповещение об атаках и проблемах в сети;

d) чтобы применялись надежные протоколы маршрутизации.

### 8.3 Уровень приложений

Требования безопасности периферийного приложения должны предусматривать:

a) чтобы в нем производилась оценка безопасности, включая проверку соответствия требованиям безопасности, управление активами, сканирование на вирусы и т. д.;

b) чтобы периферийное приложение поддерживало аутентификацию и авторизацию при взаимодействии между платформой управления облаком и другими периферийными приложениями;

c) чтобы оно защищало конфиденциальные данные, препятствуя несанкционированному доступу и подлогу данных;

d) чтобы оно поддерживало проверку интеграции периферийного приложения;

e) чтобы оно проверяло личность и полномочия администратора во время загрузки и создания экземпляров периферийного приложения;

f) чтобы оно поддерживало конфиденциальность и защиту интеграции в процессах переноса, передачи, хранения, совместного использования и уничтожения данных;

g) чтобы оно поддерживало функцию автоматической идентификации и укрепления безопасности, основанную на расширении безопасности языка программирования и статическом анализе программ;

h) чтобы оно поддерживало функции мониторинга, анализа и оповещения в режиме реального времени в отношении быстродействия приложений, трафика, исходного канала и клиентской среды;

i) чтобы оно поддерживало проверку приложений, регулярно собирало журналы событий безопасности периферийных устройств и приложений, хранило и анализировало их, а затем подавало сигналы и отслеживало нарушения, случаи превышения полномочий и аномальное поведение приложения.

## 9 Руководящие указания по средствам обеспечения безопасности для услуги периферийных вычислений

### 9.1 Уровень инфраструктуры

Для выполнения требований безопасности уровня инфраструктуры следует предусмотреть нижеперечисленные средства обеспечения безопасности:

a) мониторинг рисков безопасности данных и раннее предупреждение для предотвращения подлога и утечки данных;

b) безопасное хранение данных, включая возможности хранения в зашифрованном виде и инкапсуляции конфиденциальных данных;

c) меры защиты платформы виртуализации с помощью укрепления безопасности системы, изоляции в целях безопасности, управления защитой, шифрования данных и других мер обеспечения безопасности данных в виртуализированной сети;

d) меры безопасности для обеспечения безопасности виртуализированных сетевых функций, в том числе:

- функции управления аутентификацией;
- функции управления доступом;
- удаленная проверка безопасности системы;
- обеспечение безопасности связи;
- аттестация;
- зеркалирование;
- подпись;
- изоляция в целях безопасности;
- аппаратно-опосредованные анклавы исполнения;
- аппаратный корень доверия;
- аппаратное шифрование;
- надежная среда выполнения;
- самошифруемое хранилище данных;
- прямой доступ к оперативной памяти;
- аппаратные модули безопасности;
- защита и проверка целостности программного обеспечения.

### 9.2 Сетевой уровень

Следует предусмотреть средства обеспечения безопасности сетевого уровня, включающие, в частности:

a) средства защиты конфиденциальности и обеспечения целостности при передаче данных, такие как отметка времени, последовательные номера, шифрование линии и другие механизмы;

b) поддержку средств предотвращения перехвата сеанса, таких как шифрование трафика данных между сторонами, использование длинного случайного числа или строки в качестве ключа сеанса и повторное создание идентификатора сеанса после успешного входа в систему;

c) контроль безопасности данных для периферийных узлов, включая проверку идентичности, изоляцию в целях безопасности, непрерывный мониторинг и раннее предупреждение, шифрование данных, десенсибилизацию и резервное копирование данных;

d) надежные протоколы маршрутизации.

### 9.3 Уровень приложений

Следует предусмотреть средства обеспечения безопасности уровня приложений, включающие, в частности:

a) управление разрешениями приложения для различных пользователей и сценариев в целях обеспечения конфиденциальности, целостности и готовности данных и услуг уровня приложения;

b) защиту от вирусных атак и своевременное обновление базы данных вирусов для предотвращения утечки или кражи данных;

c) выявление и оценку конфиденциальных данных, включая авторизацию десенсибилизации, хранение данных в зашифрованном виде, мониторинг и отслеживание, оповещение о нештатных ситуациях, управление проверкой, уничтожение данных и другие меры;

d) проверку идентичности, непрерывный мониторинг и раннее предупреждение.

# Библиография


[b-ITU-T E.800] Рекомендация МСЭ-T E.800 (2008 г.), *Определение терминов, относящихся к качеству обслуживания*.

[b-ITU-T X.1811] Рекомендация МСЭ-T X.1811 (2021 г.), *Руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность*.

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

[b-ITU-R M.1645] Recommendation ITU-R M.1645 (2006), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

[b-ITU-R M.2083] Рекомендация МСЭ-R M.2083 (2015 г.), *Концепция IMT − Основы и общие задачи будущего развития IMT на период до 2020 года и далее*.

[b-3GPP TS 23.548] 3GPP 23.548 (2021), 5*G system enhancements for edge computing (version 17.2.0 release 17)*.

[b-Daniel] B. Daniel, *Is edge computing secure? Here are 4 security risks to be aware of* 9 December 2020.
https://www.trentonsystems.com/blog/is-edge-computing-secure

[b-ENISA] (ENISA) European Union Agency for Cybersecurity (2019), *ENISA Threat Landscape for 5G Networks.* December 2020. Available to:
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

# 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.