|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **Международный союз электросвязи****Бюро стандартизации электросвязи** |  |
|  | Женева, 23 апреля 2024 года |
| **Осн**.: | **Циркуляр 195 БСЭ**SG17/XY | **Кому**:– Администрациям Государств – Членов Союза**Копии**:– Членам Сектора МСЭ-Т– Ассоциированным членам МСЭ-Т, участвующим в работе 17‑й Исследовательской комиссии– Академическим организациям − Членам МСЭ– Председателю и заместителям председателя 17‑й Исследовательской комиссии МСЭ-Т− Директору Бюро развития электросвязи− Директору Бюро радиосвязи |
| **Тел**: | +41 22 730 6206 |
| **Факс**: | +41 22 730 5853 |
| **Эл. почта**: | tsbsg17@itu.int |
| **Предмет**: | **Консультации с Государствами-Членами по проектам новых Рекомендаций МСЭ-Т X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec‑5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec) и X.1820 (X.5Gsec‑srocvs), по которым сделано заключение и которые предложены для утверждения на собрании 17‑й Исследовательской комиссии МСЭ‑Т, Женева, 2–6 сентября 2024 года** |

Уважаемая госпожа,
уважаемый господин,

1 17-я Исследовательская комиссия МСЭ‑Т (Безопасность) намерена применить традиционную процедуру утверждения, описанную в разделе 9 Резолюции 1 (Пересм. Женева, 2022 г.) ВАСЭ, для утверждения упомянутых выше проектов Рекомендаций на своем следующем очном собрании, которое состоится в Женеве 2–6 сентября 2024 года. Повестка дня и вся необходимая информация, касающаяся данного собрания 17‑й Исследовательской комиссии МСЭ‑Т, будет представлена в Коллективном письме [8/17](https://www.itu.int/md/T22-SG17-COL-0008/en).

2 Название, резюме предлагаемых к утверждению проектов Рекомендаций МСЭ-Т и указание на место их размещения содержатся в **Приложении 1**.

ПРИМЕЧАНИЕ 1 БСЭ. – Ни для одного из этих текстов, по которым сделаны заключения, за исключением проекта новой Рекомендации X.1820 (X.5Gsec-srocvs), не был представлен обосновывающий документ согласно Рекомендации МСЭ-Т A.5.

ПРИМЕЧАНИЕ 2 БСЭ. – На дату настоящего Циркуляра БСЭ не получило в отношении указанных проектов текстов каких-либо заявлений в соответствии с политикой в области прав интеллектуальной собственности (ПИС). Для получения актуальной информации членам предлагается обращаться к базе данных ПИС по адресу: [www.itu.int/ipr/](http://www.itu.int/ipr/).

3 Настоящий Циркуляр открывает официальные консультации с Государствами – Членами МСЭ относительно возможности рассмотрения этих текстов с целью их утверждения на предстоящем собрании в соответствии с п. 9.4 Резолюции 1. Государствам-Членам предлагается заполнить содержащуюся в **Приложении 2** форму и вернуть ее не позднее 23 час. 59 мин. UTC **21 августа 2024 года**.

4 Если в своих ответах 70 или более процентов Государств-Членов поддержат рассмотрение с целью утверждения, то одно пленарное заседание будет посвящено применению процедуры утверждения. Государства-Члены, которые не предоставят полномочий для осуществления процедуры, должны сообщить Директору БСЭ причины такого мнения и указать, какие возможные изменения могли бы способствовать продолжению работы.

С уважением,

Сейдзо Оноэ
Директор Бюро
стандартизации электросвязи

**Приложения**: 2

ПРИЛОЖЕНИЕ 1

Резюме и указание на место размещения проектов новых Рекомендаций
МСЭ-Т X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec), X.1820 (X.5Gsec-srocvs), по которым сделано заключение

# 1 Проект новой Рекомендации МСЭ-T X X.1237 (X.tsfpp) [[R62](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0062)]

Требования безопасности для защиты информации, позволяющей установить личность, c целью противодействия спаму при передаче сообщений на мобильные устройства

**Резюме**

В настоящее время спамовый контент, который создается в коммерческих интересах (реклама), проникает в каждое средство передачи, для того чтобы его получил каждый пользователь. Операторы, разработчики программного обеспечения и другие организации изучают различные виды технологий, платформ, услуг и приложений для противодействия спаму. Однако, если при разработке и реализации этих подходов не принять во внимание защиту информации, позволяющей установить личность (PII), то это может негативно отразиться на их функциональных возможностях и эффективности.

В настоящей Рекомендации учитывается защита PII при разработке и реализации решений по борьбе со спамом при передаче сообщений на мобильные устройства. Представлен обзор процессов противодействия спаму при передаче сообщений на мобильные устройства и предложены требования безопасности с целью противодействия спаму при передаче сообщений на мобильные устройства. Кроме того, введены функции объектов и процедуры обработки.

# 2 Проект новой Рекомендации МСЭ-T X.1283 (X.gpwd) [[R66](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0066)]

Анализ угроз и руководящие указания по обеспечению безопасности решений по аутентификации с использованием пароля и без использования пароля

**Резюме**

Сообщество специалистов по компьютерной безопасности предпринимает значительные усилия по замене аутентификации с использованием пароля альтернативными решениями, которые известны как аутентификация без использования пароля. К сожалению, многие из предлагаемых решений без использования пароля имеют те же ограничения, что и существующие решения с использованием пароля. Эти решения уязвимы, среди прочего, для атак через посредника и фишинга.

В Рекомендации МСЭ-T X.1283 (X.gpwd) выполнен анализ безопасности и угроз применительно к решениям аутентификации, основанным на использовании общих секретов. Подробно рассматриваются риски безопасности, присущие системам с использованием пароля и появляющимся решениям без использования пароля.

В настоящей Рекомендации проводится анализ угроз, формируются руководящие указания и примеры передового опыта по защите пользователей и учетных записей на основе этих методов. Эта работа может быть использована специалистами для поддержки традиционных решений по мере их перевода на более строгие методы аутентификации на базе PKI (например, МСЭ-T X.1277 и МСЭ-T X.1278).

# 3 Проект новой Рекомендации МСЭ-T X.1353 (X.ztd-iot) [[R63](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0063)]

Методика обеспечения безопасности автоматического развертывания массового IoT на основе блокчейна

**Резюме**

Массовый интернет вещей (mIoT) – важное приложение будущих сетей связи. При ожидаемом разнообразии сценариев использования mIoT производителям сложно заранее снабжать выпускаемые ими устройства IoT информацией, относящейся к конкретному оператору сети подвижной связи и/или конкретной услуге (например, идентификационные данные или ключи), поскольку производителям может быть неизвестно, где и каким образом в конечном счете будут установлены и активированы их устройства. Современный подход основан на ручной настройке устройств потребителями, что приемлемо для мелкомасштабных приложений IoT. Однако для устройств mIoT указанный выше подход неприменим вследствие продолжительности, нерентабельности и трудоемкости процесса ручной настройки. Поэтому для mIoT требуется автоматическое предоставление учетных данных, называемое "без участия пользователя".

В настоящей Рекомендации представлена методика обеспечения безопасности при разработке децентрализованной системы управления учетными данными в поддержку полностью автоматического развертывания mIoT в будущем на основе блокчейна. Это один из осуществимых и многообещающих подходов к обеспечению полностью автоматического развертывания будущего массового IoT. Автоматическое развертывание позволит устройствам IoT автоматически получать учетные данные от соответствующих операторов сетей подвижной связи и поставщиков услуг и таким образом автоматически подключаться к сетям и услугам. Это значительно упростит процесс развертывания устройств mIoT в различных отраслях в будущем. В настоящей Рекомендации рассматриваются архитектура безопасности, аспекты безопасности и соответствующие процедуры ее обеспечения (аттестация, аутентификация и предоставление учетных данных устройств), которые необходимы для создания такой платформы автоматического развертывания mIoT.

# 4 Проект новой Рекомендации МСЭ-T X.1354 (X.sc-iot) [[R64](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0064)]

Средства контроля безопасности для систем IoT

**Резюме**

В Рекомендации МСЭ-T X.1354 (X.sc-iot) представлены практические руководящие указания по безопасности для трех заинтересованных сторон – поставщиков, разработчиков и пользователей услуг в системах интернета вещей (IoT), а также описаны используемые ими концепция, риски и средства контроля безопасности.

Системам IoT присущи особые проблемы в области информационной безопасности, поскольку они широко распространены и включают в себя большое количество разнообразных объектов. Это означает, что существует очень большая зона атаки и сложная задача для системы управления информационной безопасностью в применении и поддержании соответствующих средств контроля безопасности на уровне всей системы.

# 5 Проект новой Рекомендации МСЭ-T X.1384 (X.itssec-5) [[R67](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0067)]

Требования безопасности и руководящие указания по обеспечению безопасности для автомобильных периферийных вычислений

**Резюме**

В Рекомендации МСЭ-Т X.1384 (ранее X.itssec-5) представлены требования безопасности и руководящие указания по обеспечению безопасности для автомобильных периферийных вычислений (VEC). VEC – это парадигма вычислений, в которой используются возможности обработки на границе сети для распределения вычислительных ресурсов в базовом облаке в среде ИТС. Кроме того, VEC предоставляет участникам дорожного движения более локализованные услуги хранения и поддержки приложений, позволяя таким образом добиваться меньшего времени скрытых задержек, большего быстродействия, осведомленности о местоположении, высокой готовности и качества обслуживания для приложений потоковой передачи в реальном времени благодаря приближению обработки данных к транспортному средству.

VEC сопровождается многими проблемами и трудностями в области безопасности, поскольку требует более оперативной реакции на запросы услуг для конечных пользователей. В настоящей Рекомендации проведен анализ выявленных в отношении VEC угроз и уязвимостей и представлены требования безопасности для VEC. Наряду с этим приведены сценарии использования услуг VEC.

# 6 Проект новой Рекомендации МСЭ-T X.1471 (X.websec-7) [[R65](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0065)]

Монитор обращений для онлайновых аналитических услуг

**Резюме**

Услуга анализа больших данных работает с неопределенными неструктурированными данными, включая данные о поведении пользователей, их покупках, платежах, местоположении и потреблении ими различного интернет-контента. Это может выявлять новые закономерности, которые ранее не обнаруживались, и прогнозировать будущие состояния. Однако в процессе анализа возможно несанкционированное злонамеренное использование некоторых данных.

В настоящей Рекомендации описан монитор обращений для анализа больших данных и операций по обнаружению несанкционированного использования данных. В Рекомендации проведен анализ угроз и проблем безопасности в области аналитики больших данных, а также описаны требования безопасности, с помощью которых возможно смягчить эти угрозы и решить проблемы безопасности, используя механизмы управления доступом. Для того чтобы определить возможности обеспечения безопасности, необходимые для смягчения угроз безопасности и решения проблем безопасности в области аналитики больших данных, предлагается методика монитора обращений, основанная на управлении доступом.

# 7 Проект новой Рекомендации МСЭ-T X.1819 (X.5Gsec-netec) [[R60](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0060)]

Возможности обеспечения безопасности сетевого уровня для периферийных вычислений IMT‑2020/5G

**Резюме**

Периферийные вычисления для сети IMT-2020/5G (5G EC) будут играть ключевую роль в предоставлении услуг с малой задержкой и услуг по разгрузке трафика в сетях IMT последующих поколений. Ряд значимых факторов могут усложнить и увеличить риски безопасности на сетевом уровне, поддерживающем 5G EC, и даже создать новые проблемы безопасности при обеспечении сетевой безопасности. К таким факторам относятся гибкая сетевая архитектура IMT-2020/5G, переменные позиции развертывания EC, различные сценарии применения, разные типы абонентских частных сетей и сетей доступа и т. д. Границы между сетями электросвязи и частными сетями будут становиться все менее определенными, и область уязвимости будет расширяться. По этой причине следует описать требования и меры безопасности сетевого уровня, включая сети электросвязи и частные сети.

# 8 Проект новой Рекомендации МСЭ-T X.1820 (X.5Gsec-srocvs) [[R61](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0061)]

Требования безопасности функционирования базовой сети IMT-2020/5G в поддержку вертикальных услуг

**Резюме**

С развитием системы IMT-2020/5G ключевыми сценариями для IMT-2020/5G стали вертикальные услуги. В вертикальных услугах для "умных" предприятий и "умных" городов, использующих сеть IMT-2020/5G, многие пользовательские устройства обращаются к вертикальным услугам с интенсивным межмашинным обменом и сверхнадежной передачей данных с малой задержкой (URLLC).

Для поддержки сценариев вертикальных услуг, требующих URLLC, некоторые функции базовой сети IMT-2020/5G могут быть развернуты на локальных объектах, которые находятся ближе к пользователям вертикальных услуг, в то время как другие функции базовой сети IMT-2020/5G по‑прежнему развертываются на центральном объекте. В базовой сети IMT-2020/5G, работающей в таком формате развертывания, по сравнению с базовой сетью IMT-2020/5G, развернутой как одно целое, возможно возникновение специфических угроз безопасности.

Для обеспечения безопасности функционирования базовой сети IMT-2020/5G в поддержку вертикальных услуг необходимо проанализировать специфические угрозы безопасности и описать соответствующие требования безопасности.

В настоящей Рекомендации проведен анализ угроз безопасности данных, угроз безопасности сетей и угроз физической безопасности, специфических для функционирования базовой сети IMT-2020/5G, развернутой как на центральном, так и на местном объектах в поддержку вертикальных услуг, и определены соответствующие требования безопасности.

В этом проекте текста, по которому сделано заключение, перечислены нормативные ссылки, требующие обоснования согласно Рекомендации A.5 МСЭ-Т, которое представлено в SG17-[TD1739](https://www.itu.int/md/T22-SG17-240220-TD-PLEN-1739/en).

ПРИЛОЖЕНИЕ 2

Предмет: ответ Государства-Члена на Циркуляр 195 БСЭ
Консультации по проектам новых Рекомендаций МСЭ-Т X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec), X.1820 (X.5Gsec-srocvs),
по которым сделано заключение

|  |  |  |  |
| --- | --- | --- | --- |
| **Кому**: | Директору Бюро стандартизации электросвязиМеждународный союз электросвязиPlace des NationsCH 1211 Geneva 20, Switzerland | **От**: | [Фамилия][Официальная должность/титул][Адрес] |
| **Факс**:**Эл. почта**: | +41 22 730 5853tsbdir@itu.int | **Факс**:**Эл. почта**: |  |
|  |  | **Дата**: | [Место,] [Дата] |

Уважаемая госпожа,
уважаемый господин,

В рамках консультаций с Государствами-Членами по указанным в Циркуляре 195 БСЭ проектам текстов, по которым сделано заключение, я хотел/хотела бы сообщить вам мнение администрации, изложенное в таблице, ниже.

|  | **Выбрать одну из двух ячеек** |
| --- | --- |
| **Проект новой Рекомендации МСЭ-T X.1237 (X.tsfpp)** | **[ ]  Предоставляет полномочия** ИК17 для рассмотрения этого текста с целью его утверждения (в этом случае выбрать один из двух вариантов ⃝):⃝ Замечания или предлагаемые изменения отсутствуют⃝ Замечания и предлагаемые изменения прилагаются |
| [ ]  **Не предоставляет полномочий** ИК17 для рассмотрения этого текста с целью его утверждения (причины этого мнения и возможные изменения, которые могли бы способствовать продолжению работы, прилагаются) |
| **Проект новой Рекомендации МСЭ-T X.1283 (X.gpwd)** | **[ ]  Предоставляет полномочия** ИК17 для рассмотрения этого текста с целью его утверждения (в этом случае выбрать один из двух вариантов ⃝):⃝ Замечания или предлагаемые изменения отсутствуют⃝ Замечания и предлагаемые изменения прилагаются |
| [ ]  **Не предоставляет полномочий** ИК17 для рассмотрения этого текста с целью его утверждения (причины этого мнения и возможные изменения, которые могли бы способствовать продолжению работы, прилагаются) |
| **Проект новой Рекомендации МСЭ-T X.1353****(X.ztd-iot)** | **[ ]  Предоставляет полномочия** ИК17 для рассмотрения этого текста с целью его утверждения (в этом случае выбрать один из двух вариантов ⃝):⃝ Замечания или предлагаемые изменения отсутствуют⃝ Замечания и предлагаемые изменения прилагаются |
| [ ]  **Не предоставляет полномочий** ИК17 для рассмотрения этого текста с целью его утверждения (причины этого мнения и возможные изменения, которые могли бы способствовать продолжению работы, прилагаются) |
| **Проект новой Рекомендации МСЭ-T X.1354****(X.sc-iot)** | [ ]  **Предоставляет полномочия** ИК17 для рассмотрения этого текста с целью его утверждения (в этом случае выбрать один из двух вариантов ⃝):⃝ Замечания или предлагаемые изменения отсутствуют⃝ Замечания и предлагаемые изменения прилагаются |
| [ ]  **Не предоставляет полномочий** ИК17 для рассмотрения этого текста с целью его утверждения (причины этого мнения и возможные изменения, которые могли бы способствовать продолжению работы, прилагаются) |
| **Проект новой Рекомендации МСЭ-T X.1384 (X.itssec-5)** | [ ]  **Предоставляет полномочия** ИК17 для рассмотрения этого текста с целью его утверждения (в этом случае выбрать один из двух вариантов ⃝):⃝ Замечания или предлагаемые изменения отсутствуют⃝ Замечания и предлагаемые изменения прилагаются |
| [ ]  **Не предоставляет полномочий** ИК17 для рассмотрения этого текста с целью его утверждения (причины этого мнения и возможные изменения, которые могли бы способствовать продолжению работы, прилагаются) |
| **Проект новой Рекомендации МСЭ-Т X.1471 (X.websec-7)** | **[ ]  Предоставляет полномочия** ИК17 для рассмотрения этого текста с целью его утверждения (в этом случае выбрать один из двух вариантов ⃝):⃝ Замечания или предлагаемые изменения отсутствуют⃝ Замечания и предлагаемые изменения прилагаются |
| [ ]  **Не предоставляет полномочий** ИК17 для рассмотрения этого текста с целью его утверждения (причины этого мнения и возможные изменения, которые могли бы способствовать продолжению работы, прилагаются) |
| **Проект новой Рекомендации МСЭ-Т X.1819 (X.5Gsec-netec)** | **[ ]  Предоставляет полномочия** ИК17 для рассмотрения этого текста с целью его утверждения (в этом случае выбрать один из двух вариантов ⃝):⃝ Замечания или предлагаемые изменения отсутствуют⃝ Замечания и предлагаемые изменения прилагаются |
| [ ]  **Не предоставляет полномочий** ИК17 для рассмотрения этого текста с целью его утверждения (причины этого мнения и возможные изменения, которые могли бы способствовать продолжению работы, прилагаются) |
| **Проект новой Рекомендации МСЭ-T X.1820 (X.5Gsec-srocvs)** | **[ ]  Предоставляет полномочия** ИК17 для рассмотрения этого текста с целью его утверждения (в этом случае выбрать один из двух вариантов ⃝):⃝ Замечания или предлагаемые изменения отсутствуют⃝ Замечания и предлагаемые изменения прилагаются |
| [ ]  **Не предоставляет полномочий** ИК17 для рассмотрения этого текста с целью его утверждения (причины этого мнения и возможные изменения, которые могли бы способствовать продолжению работы, прилагаются) |

С уважением,

[Фамилия]
[Официальная должность/титул]
Администрация [Государства-Члена]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_