|  |  |  |
| --- | --- | --- |
|  | **Международный союз электросвязи****Бюро стандартизации электросвязи** |  |

 Женева, 11 октября 2023 года

|  |  |
| --- | --- |
| **Осн**.: **Циркуляр 142 БСЭ**SG17/XY**Тел**.: +41 22 730 6206**Факс**: +41 22 730 5853**Эл. почта**: tsbsg17@itu.int | **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 |
|  |
| **Предмет**: | **Консультации с Государствами-Членами по проектам Рекомендаций МСЭ-Т X.1150 (X.saf-dfs), X.1221 (X.stie), X.1222 (X.taeii), X.1280 (X.oob-sa), X.1281 (X.osia), Поправке 1 к X.1352, пересмотренной X.1373 и X.1818 (X.5Gsec-ctrl), по которым сделано заключение и которые предложены для утверждения на собрании 17‑й Исследовательской комиссии МСЭ‑Т, 20 февраля – 1 марта 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 собрании, которое состоится в Южно-Африканской Республике 20 февраля – 1 марта 2024 года. Повестка дня и вся необходимая информация, касающаяся данного собрания 17‑й Исследовательской комиссии МСЭ‑Т, будет представлена в Коллективном письме [6/17](https://www.itu.int/md/T22-SG17-COL-0006/en).

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

ПРИМЕЧАНИЕ 1. – Ни для одного из этих текстов, по которым сделаны заключения, за исключением проектов новых Рекомендаций X.1221 (X.stie) и X.1222 (X.taeii), не был представлен обосновывающий документ согласно Рекомендации A.5 МСЭ-Т.

ПРИМЕЧАНИЕ 2. – 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 **8 февраля 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 Рекомендаций
МСЭ-Т X.1150 (X.saf-dfs), X.1221 (X.stie), X.1222 (X.taeii), X.1280 (X.oob-sa), X.1281 (X.osia), Поправки 1 к X.1352, пересмотренной X.1373 и X.1818 (X.5Gsec-ctrl), по которым сделано заключение

# 1 Проект новой Рекомендации МСЭ-T X.1150 (X.saf-dfs) [[R50](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0050)]

Система обеспечения безопасности цифровых финансовых услуг

Резюме

Цифровые финансовые услуги (ЦФУ) образуют сложную экосистему с участием различных заинтересованных сторон, таких как банки, поставщики ЦФУ, операторы сетей подвижной связи (MNO), поставщики платформ ЦФУ, регуляторные органы, агенты, торговые компании, поставщики платежных услуг, производители устройств, разработчики приложений, поставщики услуг меток безопасности, производители оригинального оборудования (OEM) и клиенты. Взаимосвязь этих объектов и зависимость от нескольких сторон в экосистеме расширяет границы безопасности, которые охватывают не только поставщиков ЦФУ, но также клиентов, поставщиков сетей, производителей мобильных телефонов и других сторонних поставщиков в экосистеме.

Система обеспечения безопасности ЦФУ предоставляет обзор угроз безопасности и уязвимостей, с которыми сталкиваются соответствующие заинтересованные стороны ЦФУ. Регуляторные органы, в том числе органы в области электросвязи, банковской системы и платежных систем, также могут использовать систему обеспечения безопасности ЦФУ, с тем чтобы устанавливать базовые уровни безопасности для поставщиков ЦФУ.

Эта система, после ее реализации, дополнит устоявшуюся практику управления рисками и информационной безопасностью заинтересованных сторон, участвующих в экосистеме ЦФУ. Например, меры безопасности, приведенные в настоящей Рекомендации, могут быть включены в программу безопасности информационно-коммуникационных технологий (ИКТ) поставщика ЦФУ.

В настоящей Рекомендации описана система обеспечения безопасности ЦФУ, которая обеспечивает систематический процесс управления рисками безопасности для оценки угроз и уязвимостей и определяет соответствующие меры безопасности, которые должны быть реализованы заинтересованными сторонами ЦФУ. Угрозы, связанные с торговыми компаниями, поставщиками платежных услуг и другими организациями финансовых услуг, а также конкретные способы смягчения последствий угроз, с которыми они сталкиваются, выходят за рамки настоящей Рекомендации.

В состав системы обеспечения безопасности ЦФУ входят следующие компоненты:

a) процесс управления рисками безопасности, основанный на [b-ISO/IEC 27005];

b) оценка угроз и уязвимостей в отношении базовой инфраструктуры оператора сети подвижной связи и поставщика ЦФУ, приложений ЦФУ, услуг, сетевых операций и сторонних поставщиков, участвующих в экосистеме предоставления ЦФУ;

c) стратегии смягчения последствий, которые основаны на результатах оценок, указанных в подпункте b), выше. Меры по смягчению последствий определяют 119 средств обеспечения безопасности применительно к угрозам безопасности, которые описаны в разделе 13 настоящей Рекомендации.

# 2 Проект новой Рекомендации X.1221 (X.stie), [[R47](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0047)]

Структурированное представление информации об угрозах (STIX)

Резюме

В настоящей Рекомендации определено структурированное представление информации об угрозах (STIX) – язык, используемый для описания объектов данных и обмена аналитической информацией о киберугрозах, а также формат сериализации JSON. STIX не опирается на какой-либо конкретный транспортный механизм. Настоящая Рекомендация технически эквивалентна и совместима с опубликованным стандартом OASIS STIX 2.1 [b-STIX v2.1].

# 3 Проект новой Рекомендации X.1222 (X.taeii) [[R48](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0048)]

Надежный автоматический обмен аналитической информацией об угрозах (TAXII)

Резюме

Настоящая Рекомендация представляет собой протокол прикладного уровня для передачи информации о киберугрозах простым и масштабируемым способом. В этой спецификации определен интерфейс прикладного программирования (API) TAXII REST и его ресурсы, а также требования к реализациям клиента и сервера TAXII. TAXII представляет собой набор методов совместного использования и передачи объектов данных, относящихся к обмену аналитической информацией о киберугрозах. Настоящая Рекомендация технически эквивалентна и совместима с опубликованным стандартом OASIS TAXII версии 2.1 [b-TAXII v2.1].

# 4 Проект новой Рекомендации X.1280 (X.oob-sa) [[R51](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0051)]

Структура внеполосной аутентификации сервера с использованием мобильных устройств

Резюме

В стандартах технологии аутентификации устойчивость к имперсонации верификатора рассматривается как требование наивысшего уровня гарантии аутентификации. Однако существующие технологии аутентификации ориентированы на аутентификацию пользователя, поэтому существует ограничение, которое заключается в невозможности провести явную проверку поставщика услуг.

В настоящей Рекомендации представлена структура внеполосной аутентификации сервера с использованием мобильных устройств, которая устраняет уязвимость, связанную с имперсонацией верификатора, и ограничение, связанное с зависимостью существующих аутентификаторов от пользовательского терминала. Эта структура дает пользователю возможность предоставлять информацию аутентификации пользователя после явной и независимой проверки поставщика услуг в процессе аутентификации пользователя на любых пользовательских терминалах.

# 5 Проект новой Рекомендации X.1281 (X.osia) [[R52](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0052)]

API для функциональной совместимости систем управления определением идентичности

Резюме

В настоящей Рекомендации описан набор стандартизованных интерфейсов прикладного программирования (API), необходимых для соединения нескольких структурных блоков решения по управлению определением идентичности.

# 6 Проект новой Поправки 1 к Рекомендации X.1352 [[R49](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0049)]

Требования безопасности для устройств и шлюзов интернета вещей

Резюме

В Рекомендации МСЭ-Т X.1352 установлены детальные требования по пяти аспектам безопасности, применимым к устройствам и шлюзам интернета вещей (IoT): аутентификация, криптография, безопасность данных, безопасность платформы устройств и физическая безопасность. Эти требования основаны на эталонной модели IoT, которая определена в Рекомендации МСЭ-T Y.4100, и структуре безопасности IoT, которая определена в Рекомендации МСЭ-T X.1361.

Аспект аутентификации включает аутентификацию пользователя, безопасное использование учетных данных для аутентификации и аутентификацию устройств. Аспект криптографии включает использование безопасных криптографических алгоритмов, безопасное управление ключами и безопасное генерирование случайных чисел. Аспект безопасности данных охватывает безопасную передачу и хранение данных, управление информационными потоками, безопасное управление сеансами и управление информацией, позволяющей установить личность (PII). Аспект безопасности платформы устройств включает пять элементов: безопасное программное обеспечение, безопасное обновление, управление безопасностью, ведение журналов событий и проставление отметок времени. Аналогично аспект физической безопасности включает безопасный физический интерфейс и защиту от несанкционированного доступа.

# 7 Проект пересмотренной Рекомендации X.1373 [[R53](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0053)]

Возможность безопасного обновления программного обеспечения для устройств связи в интеллектуальных транспортных системах

Резюме

По мере развития технологий интеллектуальных транспортных систем (ИТС) связь между транспортным средством и другим объектом, например связь транспортного средства с транспортным средством (V2V) и транспортного средства с инфраструктурой (V2I), становится все более распространенной. Устанавливаемые на транспортных средствах электротехнические устройства, такие как электронные блоки управления (ECU), системы автоматического взимания платы (ETC) и автомобильные навигационные системы, постоянно усложняются. В результате для устранения ошибок, повышения производительности и безопасности во избежание аварий требуется соответствующее обновление программных модулей, которыми оснащены эти электротехнические устройства.

Для выполнения указанных выше требований в Рекомендации МСЭ‑Т X.1373 представлены процедуры безопасного обновления программного обеспечения между сервером обновления программного обеспечения и транспортными средствами с соответствующими средствами контроля безопасности, включая сообщения бортовой системы связи. На практике настоящая Рекомендация может использоваться в автомобильной промышленности и отраслях, связанных с ИТС, в качестве набора стандартных возможностей для передового опыта.

# 8 Проект новой Рекомендации X.1818 (X.5Gsec-ctrl) [[R46](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0046)]

Средства контроля безопасности для эксплуатации и обслуживания сетевых систем IMT-2020/5G

Резюме

В настоящей Рекомендации представлено всестороннее руководство по обеспечению безопасности системы IMT-2020 (также называемой 5G) на этапах эксплуатации и обслуживания. Описанные угрозы безопасности и рекомендуемые средства контроля безопасности являются результатом анализа угроз.

Настоящая Рекомендация посвящена автономной системе 5G (SA 5G), а также виртуальной инфраструктуре и связанным с ней системам управления, которые, как ожидается, будут служить основой для развертывания 5G. Кроме того, внимание уделяется не только технологиям, но также человеческим и технологическим аспектам, влияющим на безопасность услуг 5G. Рекомендуемые меры безопасности описаны на высоком уровне и в надлежащих случаях приведены ссылки на установленные стандарты и передовой опыт.

ПРИЛОЖЕНИЕ 2

Предмет: ответ Государства-Члена на Циркуляр 142 БСЭ
Консультации по проектам Рекомендаций МСЭ-Т X.1150 (X.saf-dfs),
X.1221 (X.stie), X.1222 (X.taeii), X.1280 (X.oob-sa), X.1281 (X.osia), Поправке 1 к X.1352, пересмотренной X.1373 и X.1818 (X.5Gsec-ctrl), 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 142 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.1150****(X.saf-dfs)** | **[ ]  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.1221****(X.stie)** | **[ ]  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.1222 (X.taeii)** | **[ ]  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.1280** **(X.oob-sa)** | [ ]  **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.1811** **(X.osia)** | [ ]  **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 Поправки к Рекомендации МСЭ-Т X.1352**  | **[ ]  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 пересмотренной Рекомендации МСЭ-Т X.1373** | **[ ]  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.1818** **(X.5Gsec-ctrl)** | **[ ]  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]