|  |  |
| --- | --- |
| **Всемирная ассамблея по стандартизации электросвязи (ВАСЭ-20)Женева, 1–9 марта 2022 года** |  |
|  |  |
| **ПЛЕНАРНОЕ ЗАСЕДАНИЕ** | Документ 20-R |
|  | **Декабрь 2021 года** |
|  | **Оригинал: английский** |
|  |
| 17-я Исследовательская комиссия МСЭ-Т |
| безопасность |
| ОТЧЕТ ИК17 МСЭ-Т ВСЕМИРНОЙ АССАМБЛЕЕ ПО СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ (васэ-20): ЧАСТЬ II – ВОПРОСЫ, ПРЕДЛАГАЕМЫЕ ДЛЯ ИССЛЕДОВАНИЯ В ходе ИССЛЕДОВАТЕЛЬСКОГО ПЕРИОДА 2022−2024 годов |

|  |  |
| --- | --- |
| **Резюме**: | В настоящем вкладе содержится отчет 17-й Исследовательской комиссии МСЭ-Т для ВАСЭ-20 о деятельности в исследовательском периоде 2017−2021 годов. |
| **Для контактов**: | Хён-Юл Юм (Heung Youl Youm)Председатель ИК17 МСЭ-ТКорея (Республика) | Эл. почта: hyyoum@sch.ac.kr |

**Примечание БСЭ**:

Отчет 17-й Исследовательской комиссии для ВАСЭ-20 представлен в следующих документах:

Часть I: **Документ 19** – Общая информация

Часть II: **Документ 20** – Вопросы, предлагаемые для исследования в ходе исследовательского периода 2022−2024 годов

Введение

В настоящем документе содержится текст Вопросов, согласованных 17‑й Исследовательской комиссией для представления ВАСЭ-20.

В таблице 1 перечислены Вопросы и указана их связь с действующим комплексом Вопросов, которые КГСЭ одобрила на своем собрании, состоявшемся 11−18 января 2021 года.

Таблица 1 − Соответствие действующих Вопросов ИК17 (одобренных, слева)
и предыдущих (справа)

| Номер | Название Вопроса | Статус | Прежний номер | Прежнее название Вопроса |
| --- | --- | --- | --- | --- |
| 1/17 | Стратегия и координация стандартизации в области безопасности | Продолжен | 1/17 | Стратегия и координация стандартизации в области безопасности |
| 2/17 | Архитектура безопасности и безопасность сетей | Продолжен | 2/17 | Архитектура безопасности и безопасность сетей |
| 3/17 | Управление безопасностью информации, передаваемой с помощью электросвязи, и услуги по обеспечению безопасности | Продолжен | 3/17 | Управление безопасностью информации, передаваемой с помощью электросвязи, и услуги по обеспечению безопасности |
| 4/17 | Кибербезопасность и противодействие спаму | Продолжен | 4/17 | Кибербезопасность и противодействие спаму |
| 6/17 | Безопасность услуг электросвязи и интернета вещей | Продолжен | 6/17 | Безопасность услуг электросвязи и интернета вещей |
| 7/17 | Безопасные прикладные услуги | Продолжен | 7/17 | Безопасные прикладные услуги |
| 8/17 | Безопасность облачных вычислений и инфраструктуры больших данных | Продолжен | 8/17 | Безопасность облачных вычислений и инфраструктуры больших данных |
| 10/17 | Архитектура и механизмы управления определением идентичности и телебиометрии | Продолжен | 10/17 | Архитектура и механизмы управления определением идентичности и телебиометрии |
| 11/17 | Общие технологии (например, Справочник, PKI, формальные языки, идентификаторы объекта) для поддержки безопасные приложения | Продолжен | 11/17 | Общие технологии (например, Справочник, PKI, формальные языки, идентификаторы объекта) для поддержки безопасные приложения |
| 13/17 | Безопасность интеллектуальных транспортных систем | Продолжен | 13/17 | Безопасность интеллектуальных транспортных систем |
| 14/17 | Безопасность технологии распределенного реестра (DLT) | Продолжен | 14/17 | Безопасность технологии распределенного реестра (DLT) |
| 15/17 | Безопасность для/с помощью появляющихся технологий, включая квантовую безопасность | Продолжен | 15/17 | Безопасность для/с помощью появляющихся технологий, включая квантовую безопасность |

Формулировка Вопросов

Вопрос 1/17

Стратегия и координация стандартизации в области безопасности

(Продолжение Вопроса 1/17)

### 1 Обоснование

Угрозы безопасности инфраструктуры электросвязи и информационно-коммуникационных технологий (ИКТ) постоянно усложняются. Предпринимаемые в течение нескольких лет усилия по защите инфраструктуры носили в определенной степени разрозненный и противодействующий характер и до настоящего времени не обеспечили желаемого уровня своевременной защиты от угроз. Атаки и угрозы вызывали значительные экономические последствия и приводили к финансовым и организационным потерям для правительств и предприятий. Для борьбы с такими угрозами важнейшее значение имеет масштабная, постоянная и целенаправленная деятельность.

Эта деятельность носит комплексный характер и требует участия большого числа организаций, занимающихся различными аспектами безопасности, каждая в рамках своей компетенции и мандата. Для осуществления такой деятельности необходима координация, сотрудничество и взаимодействие между различными заинтересованными сторонами, что является сложной и нетривиальной задачей.

Сфера охвата связанных с безопасностью вопросов весьма широка. Проблема безопасности касается практически всех аспектов ИКТ и сетей. Существуют разные подходы к выполнению требований безопасности, к числу которых относятся нижеследующие.

− Подход "снизу вверх" – эксперты разрабатывают меры безопасности для укрепления и защиты отдельного домена сети с использованием конкретных контрмер и методов, таких как биометрия и криптография. При том что этот подход довольно широко используется, он является фрагментарным и нередко приводит к несогласованному определению и применению мер безопасности.

− Подход "сверху вниз" – стратегический метод высокого уровня для решения вопросов безопасности. Для такого подхода требуется знание общей ситуации. Как правило, это более сложный подход, так как труднее найти экспертов, которые имеют полное представление о каждой части сети и требованиях к ее безопасности, чем экспертов, обладающих углубленными знаниями в одной-двух конкретных областях.

− Сочетание подходов "снизу вверх" и "сверху вниз" при координации, направленной на соединение различных частей. Часто этот метод вызывал многочисленные проблемы, обусловленные различными интересами и целями.

Данный Вопрос обеспечивает большой объем итоговых документов, которые МСЭ-Т считает важными для продвижения своей работы и достижения результатов работы. Они также являются ценными ресурсами для МСЭ и внешних организаций. К числу примеров относятся Дорожная карта по стандартам безопасности, Руководство по безопасности, Сборники материалов по безопасности и отчет "Эффективное использование стандартов безопасности". В рамках данного Вопроса будет разработана концепция и предложена организационная архитектура ИК17. Основное внимание при этом будет по-прежнему уделяться координации и организации всех направлений деятельности по безопасности электросвязи/ИКТ в рамках МСЭ-Т, а также будут и далее разрабатываться и поддерживаться документы, помогающие в деятельности по координации и налаживанию контактов. Подход "сверху вниз" к обеспечению безопасности будет использоваться в сотрудничестве с другими исследовательскими комиссиями и организациями по разработке стандартов (ОРС). Эта деятельность направлена на обеспечение более целенаправленных усилий на уровне проектов и стратегическом уровне как в рамках ИК17, так и вне ее. Данный Вопрос поддерживает виды деятельности ИК17, с тем чтобы они соответствовали эффективному процессу, позволяющему разрабатывать высококачественные, своевременные и ориентированные на рынок стандарты электросвязи/ИКТ. В рамках настоящего Вопроса также рассматриваются потребности развивающихся стран и региональных групп исследовательских комиссий путем выполнения Резолюции 44 ВАСЭ о преодолении разрыва в стандартизации.

Стратегия стандартизации безопасности – одна из важнейших тем для всех Вопросов ИК17. ИК17 необходимо рассмотреть вопрос о том, как архитектура и технологическая схема стандартизации безопасности могут улучшить разработку существующих и будущих направлений работы в области безопасности.

Основой для работы ИК17 в области безопасности являются Резолюции: 2, 7, 11, 18, 32, 40, 44, 50, 52, 54, 58, 64, 65, 67, 73, 75, 76, 77, 78, 80, 84, 86, 89, 90, 92, 93, 94, 96, 97 и 98; Резолюции 101, 123, 130, 136, 174, 177, 178, 179, 181; 188, 189, 197, 199, 200, 201, 204, 205 и 206 ПК; и Резолюции 30, 34, 43, 45, 47, 63, 67, 69, 79, 80 и 84 ВКРЭ.

ИК17 также поддерживает Направление деятельности C5 ВВУИО "Укрепление доверия и безопасности при использовании ИКТ" и Задачу 2 Плана действий Буэнос-Айреса, принятого на Всемирной конференции по развитию электросвязи 2017 года "Современная и безопасная инфраструктура электросвязи/ИКТ: Содействовать развитию инфраструктуры и услуг, в том числе формированию доверия и обеспечению безопасности при использовании электросвязи/ИКТ".

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Технические отчеты: TR.sec-manual, TR.Suss.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.arch-design.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Каковы результаты деятельности по данному Вопросу?

b) Каковы процессы, виды работы, методы работы и сроки для достижения намеченных результатов деятельности по этому Вопросу?

c) Какие документы, предназначенные для внешних пользователей (дорожная карта, сборники материалов по безопасности, Технические отчеты, информационные письма, веб-страницы и т. д.), необходимо будет разрабатывать и сопровождать МСЭ?

d) Какие необходимы семинары-практикумы по безопасности и каким образом они могут быть организованы?

e) Что требуется для установления эффективных отношений с другими ОРС с целью продвижения работы по обеспечению безопасности?

f) Каковы основные этапы, критерии успешной работы и поддерживающие показатели эффективности?

g) Каким образом возможно стимулировать интерес Членов Сектора и администраций к работе в области безопасности и каким образом сохранить импульс?

h) Каким образом сделать функции безопасности электросвязи/ИКТ более актуальными для рынка?

i) Каким образом возможно наиболее эффективно информировать правительства и частный сектор о первостепенной значимости безопасности и неотложной потребности в защите глобальных экономических интересов, которые зависят от наличия прочной и безопасной инфраструктуры электросвязи/ИКТ?

j) Какие виды деятельности в области безопасности разрабатываются в настоящее время другими исследовательскими комиссиями МСЭ и другими ОРС?

k) Каким образом удовлетворить потребности развивающихся стран и региональных групп исследовательских комиссий путем выполнения Резолюции 44 ВАСЭ?

l) Какова стратегия стандартизации, поддерживающая комплексное и согласованное решение в области безопасности электросвязи?

m) Каким образом следует учитывать существующие Рекомендации по безопасности в стратегия стандартизации?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Выполнение роли основного контакта в ИК17 по вопросам координации работы в области безопасности электросвязи/ИКТ.

b) Разработка и поддержание дорожной карты по организационной структуре, которая содержит концепцию и подробный план, определяющий уровень и объем области безопасности для исследований. В дорожной карте будут определены все соответствующие компоненты (структура, процессы) и их взаимосвязи, участвующие организации и их роли. Необходимо провести различие между появляющимися системами/сетями и существующими системами/сетями.

c) Поддержка и обновление "Дорожной карты по стандартам безопасности ИКТ".

d) Поддержка и обновление Сборников материалов по безопасности МСЭ-Т.

e) Содействие в поддержании и ведении Руководства по безопасности, опубликованного как Технический отчет "Безопасность в области электросвязи и информационных технологий", и представить соответствующий вклад в БСЭ.

f) Поддержка и обновление Технического отчета "Эффективное использование стандартов безопасности".

g) Обеспечение руководства по реализации стандартов безопасности электросвязи/ИКТ.

h) Содействие взаимодействию и сотрудничеству между группами, работающими в области разработки стандартов безопасности электросвязи/ИКТ.

i) Рассмотрение Рекомендаций и заявлений о взаимодействии от других исследовательских комиссий и ОРС, в соответствующих случаях, для оценки воздействия координации деятельности в области безопасности.

j) Содействие мерам по обеспечению эффективной координации деятельности в области безопасности, когда это необходимо.

k) Помощь в направлении заявлений о взаимодействии от внешних групп в адрес соответствующих исследовательских комиссий в МСЭ-Т.

l) Выполнение ведущей роли в МСЭ-Т при организации и планировании практикумов и семинаров по вопросам безопасности, в соответствующих случаях.

m) Обеспечение эффективного и действенного участия в работе по координации деятельности в области безопасности с другими организациями.

n) Помощь в повышении эффективности работы ИК17 (например, путем создания шаблонов, инструментов, процедур или показателей эффективности).

o) Рекомендовать национальным органам и операторам из развивающихся стран в регионах работать совместно и вносить больший вклад в деятельность ИК17 МСЭ-Т в соответствии с мандатом ИК17 и во исполнение Рекомендаций ИК17 по безопасности.

p) Оказание помощи ИК17 в преодолении разрыва в стандартизации с целью выполнения Резолюции 44 ВАСЭ, Резолюции 123 ПК и Резолюции 47 ВКРЭ.

q) Обеспечение эффективного и действенного участия в работе по координации деятельности в области безопасности в рамках ИК17, с тем чтобы обеспечить отражение в программе работы ИК17 деятельности в области безопасности, проводимой в настоящее время ИК17, и учет проблем Членов МСЭ-Т.

r) Разработка всеобъемлющего комплекта документов по стратегии стандартизации в области безопасности, включая документы по архитектуре, для поддержки стандартизации решений по безопасности во взаимодействии с другими организациями по разработке стандартов и исследовательскими комиссиями МСЭ-Т.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 ([Достойная работа и экономический рост](http://www.un.org/development/desa/disabilities/envision2030-goal8.html)),
9 ([Индустриализация, инновации и инфраструктура)](http://www.un.org/development/desa/disabilities/envision2030-goal9.html),
17 (Партнерства для достижения Цели)

Рекомендации:

Серия X и другие Рекомендации, касающиеся безопасности электросвязи/ИКТ

Вопросы:

Вопросы МСЭ-Т: 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 и 15/17

Исследовательские комиссии:

МСЭ-D; МСЭ-R; ИК 2, 3, 5, 9, 11, 13, 15, 16 и 20 МСЭ-Т; КГСЭ, включая соответствующие JCA и ОГ

Органы по стандартизации:

Альянс по решениям в отрасли электросвязи (ATIS); Альянс "За облачную безопасность" (CSA); Европейский институт стандартизации электросвязи (ЕТСИ); Институт инженеров по электротехнике и радиоэлектронике (IEEE); Целевая группа по инженерным проблемам интернета (IETF); ПК6 и ПК27 ОТК1 ИСО/МЭК, ТК292 ИСО, КТУ ИСО; Организация по развитию стандартов структурированной информации (ОРССИ); Проект партнерства третьего поколения (3GPP); Второй проект партнерства третьего поколения (3GPP2); Азиатско-Тихоокеанская программа по стандартизации (ASTAP)

Другие органы:

Европейское агентство по безопасности сетей и информации (ENISA); Национальный институт стандартов и технологий (NIST); one M2M; Региональный азиатский форум по безопасному обмену информацией (RAISE)

Вопрос 2/17

Архитектура безопасности и безопасность сетей

(Продолжение Вопроса 2/17)

### 1 Обоснование

Рекомендации МСЭ-Т X.800, X.802 и X.803 посвящены безопасности в контексте открытых систем. Архитектура безопасности для систем, обеспечивающих сквозную связь, представлена в Рекомендации МСЭ-Т X.805. Создан полный набор детально проработанных структур безопасности, охватывающий такие аспекты безопасности, как аутентификацию, контроль доступа, предотвращение отказа от авторства, конфиденциальность, целостность, а также проверку безопасности и аварийные сигналы безопасности (Рекомендации X.810, X.811, X.812, X.813, X.814, X.815 и X.816). Для обеспечения общей безопасности верхних уровней (GULS) были разработаны Рекомендации МСЭ-Т X.830, X.831, X.832, X.833, X.834 и X.835. В сотрудничестве с ПК27 ОТК1 ИСО/МЭК созданы Рекомендации МСЭ-Т X.841, X.842 и X.843 по информационным объектамбезопасностииуслугамдовереннойтретьейстороны.

Необходимо проводить постоянную работу по поддержанию и ведению, а также совершенствованию этих Рекомендаций по вопросам безопасности, с тем чтобы соответствовать потребностям новых технологий (например, сети последующих поколений (СПП), аспекты безопасности организации сетей с программируемыми параметрами (SDN)/визуализации сетевых функций (NFV), нарезка сетей (NS), цепочка функций услуг (SFC), периферийные вычисления в режиме множественного доступа (MEC), долгосрочное развитие/развитие системной архитектуры (LTE/SAE), сеть IMT-2020/5G и далее, общая структура и архитектура безопасности для услуг и приложений, основы искусственного интеллекта (ИИ)/машинного обучения (ML) в поддержку укрепления доверия и безопасности при использовании ИКТ, руководство по технической реализации систем, обеспечивающих сквозную связь, и сети на базе протокола Интернет) и услуг. Эта работа отражена в Рекомендациях X.1035 и X.1036, в которых приведены подробные сведения о протоколах обмена ключами с аутентификацией по паролю, а также о распространении и обеспечении выполнения политики; X.1037, в которой приведены руководящие указания по безопасности IPv6; X.1038, X.1042, X.1043 и X.1044, в которых приведены требования безопасности и т. д. организации сетей с программируемыми параметрами (SDN) и виртуализации сетей (NFV); X.1045, которая посвящена специализированным услугам по обеспечению безопасности на базе цепочки функций услуг (SFC).

Сети операторов электросвязи и соответствующие информационные системы подвергаются угрозам безопасности новых типов, которые обусловлены конвергенцией и мобильностью. Злоумышленники имеют более глубокий доступ к сетям, и им не требуется очень больших умений, а возможность повреждений существенно повышается. Вирусы, взломы и атаки типа отказа в обслуживании стали повсеместно распространенными и отрицательно воздействуют как на сетевые элементы, так и на вспомогательные системы.

Отрасль информационно-коммуникационных технологий ведет поиск экономически эффективных комплексных решений в области безопасности, которые не зависят от технологии и обеспечивают защиту широкого спектра сетей, услуг и приложений. Для обеспечения таких решений в среде с участием многих поставщиков безопасность сетей должна быть предусмотрена в проектном решении и оптимизирована во всех стандартных архитектурах безопасности и стандартных технологиях безопасности. Принимая во внимание угрозы безопасности среды электросвязи и отмечаемый в настоящее время прогресс в контрмерах в области безопасности, направленных против угроз, следует рассмотреть новые требования к безопасности и решения в области безопасности. Для обеспечения всеобъемлющей безопасности появляющихся сетей, услуг и приложений необходимы новые Рекомендации, показывающие, каким образом сочетать технологические стандарты и структуры безопасности.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации и Добавления: X.800, X.802, X.803, X.805, X.810, X.811, X.812, X.813, X.814, X.815, X.816, X.830, X.831, X.832, X.833, X.834, X.835, X.841, X.842, X.843, X.1011, X.1031, X.1032, X.1033, X.1034, X.1035, X.1036, X.1037, X.1038, X.1039, X.1040, X.1041, X.1042, X.1043, X.1044, X.1045, X.1046, X.1047, X.1811 и Добавления X.Suppl.2, X.Suppl.3, X.Suppl.15, X.Suppl.16, X.Suppl.23 и X.Suppl.30.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.5GSec-ecs, X.5GSec-guide, X.5Gsec-message, X.5Gsec-netec, X.5Gsec-ssl, X.5Gsec-t (X.1812), X.5Gsec-vs, TR.zt-acp и XSTP‑5Gsec‑RM.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Какое определение следует дать всеобъемлющему и согласованному решению по обеспечению безопасности электросвязи?

b) Какова архитектура комплексного и согласованного решения по обеспечению безопасности электросвязи?

c) Какова структура для применения архитектуры безопасности с целью разработки нового решения по обеспечению безопасности?

d) Какова структура для применения архитектуры безопасности с целью оценки (и последующего усовершенствования) существующего решения по обеспечению безопасности?

е) Каковы основы архитектуры для обеспечения безопасности?

i) Что такое архитектура обеспечения сквозной безопасности?

ii) Что такое архитектура безопасности открытых систем?

iii) Что такое архитектура безопасности для среды подвижной связи?

iv) Что такое архитектура безопасности для развивающихся сетей?

v) Что такое архитектура безопасности для прикладных услуг, в сотрудничестве с Вопросом 7/17?

f) Какие новые Рекомендации по вопросам архитектуры и структуры безопасности могут потребоваться для обеспечения решений в области безопасности в изменяющейся среде?

g) Какова должна быть структура стандартов архитектуры с учетом существующих Рекомендаций по безопасности?

h) Какова должна быть структура стандартов архитектуры с учетом существующих передовых технологий в области обеспечения безопасности?

i) Какие изменения следует внести в Рекомендации по структуре обеспечения безопасности, чтобы адаптировать их к появляющимся технологиям, и какие новые основополагающие Рекомендации могут потребоваться?

j) Каков порядок применения услуг по обеспечению безопасности для предоставления решений в области безопасности?

k) Каков порядок применения мониторинга инфраструктуры электросвязи/ИКТ для предоставления решений в области безопасности?

l) Каковы основы искусственного интеллекта (ИИ)/машинного обучения (ML) в поддержку укрепления доверия и безопасности при использовании ИКТ?

m) Каковы новые угрозы и проблемы безопасности, связанные с появляющимися сетевыми технологиями (например, SDN, NFV, нарезка сетей, SFC, MEC, LTE/SAE, сеть IMT‑2020/5G и далее и т. д.)?

n) Каковы требования безопасности сети IMT-2020/5G и далее, и каким образом ИК17 может обеспечить их выполнение?

o) Каковы общие механизмы безопасности для появляющихся сетевых технологий?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Разработка всеобъемлющего комплекта Рекомендаций по вопросам архитектуры и структуры безопасности для предоставления стандартных решений по обеспечению безопасности электросвязи в сотрудничестве с другими организациями по разработке стандартов и исследовательскими комиссиями МСЭ-Т.

b) Исследования и разработка Рекомендаций по надежной архитектуре сетей электросвязи, включающей передовые технологии обеспечения безопасности.

c) Исследования и разработка Рекомендаций по основам ИИ/МО в поддержку укрепления доверия и безопасности при использовании ИКТ.

d) Поддержание и ведение, а также усовершенствование Рекомендаций и Добавлений серии X.800 и серии X.103x.

e) Исследования и разработка Рекомендаций по общей безопасности сетей.

f) Исследование требований безопасности сети IMT-2020/5G и далее, координация соответствующей работы, проводимой в рамках различных Вопросов ИК17, выполнение функций основного контакта в ИК17 по аспектам безопасности сети IMT-2020/5G и далее, а также руководство исследованием и разработкой стандартов по аспектам безопасности сети IMT-2020/5G и далее.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 ([Достойная работа и экономический рост](http://www.un.org/development/desa/disabilities/envision2030-goal8.html)),
9 ([Индустриализация, инновации и инфраструктура)](http://www.un.org/development/desa/disabilities/envision2030-goal9.html),
11 ([Устойчивые города и населенные пункты](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Рекомендации:

Серия X и другие Рекомендации, касающиеся безопасности

Вопросы:

Вопросы МСЭ-Т: 1/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 и 15/17

Исследовательские комиссии:

ИК2 МСЭ-D; РГ 6B МСЭ-R; ИК 2, 9, 11, 13, 15, 16 МСЭ-Т и JCA-IMT2020

Органы по стандартизации:

Альянс по решениям в отрасли электросвязи (ATIS); Европейский институт стандартизации электросвязи (ЕТСИ); Ассоциация GSM (GSMA); Форум по неправомерному международному доступу к сети (FIINA); ПК27 и ПК37 ОТК1 ИСО/МЭК; ТК25 МЭК; ТК12 ИСО; Целевая группа по инженерным проблемам интернета (IETF); Проект партнерства третьего поколения (3GPP)

Вопрос 3/17

Управление безопасностью информации, передаваемой с помощью электросвязи, и услуги по обеспечению безопасности

(Продолжение Вопроса 3/17)

### 1 Обоснование

Для организаций электросвязи информация и вспомогательные процессы, объекты электросвязи, сети и средства передачи являются важными производственными ресурсами электросвязи. С тем чтобы организации электросвязи могли надлежащим образом управлять этими производственными ресурсами и грамотно вести коммерческую деятельность, важнейшее значение имеет управление безопасностью информации. В связи с этим была разработана Рекомендация МСЭ-Т X.1051, в которой содержатся свод правил управления безопасностью информации для организаций электросвязи.

На основе этого свода правил также были разработаны подробные и конкретные области управления, включая риски, активы, общее управление, структуру управления и инциденты, а также представлен передовой опыт в Добавлении. Следует далее изучить новые области в связи с Рекомендацией МСЭ-Т X.1051. В то же время необходимо поддерживать и обновлять эту серию Рекомендаций, отражая последние вопросы управления безопасностью информации. Цель состоит в том, чтобы на основе Рекомендации МСЭ-Т X.1051 разработать в МСЭ-Т комплект Рекомендаций по управлению безопасностью в сфере электросвязи.

Параллельно с разработкой Рекомендаций по подробным и конкретным областям управления на основе Рекомендации МСЭ-T X.1051 следует рассмотреть новые области услуг по обеспечению безопасности электросвязи и ИКТ, например услуги центров киберзащиты (CDC), включая услуги центров обеспечения безопасности (SOC), внешние услуги по обеспечению безопасности информации (MSS) и услуги групп реагирования на компьютерные инциденты (CIRT), управление жизненным циклом для средств контроля безопасности и эффективного управления рисками, а также управление информацией, позволяющей установить личность, которые требуют срочных и глобальных мер противодействия. Эти области относятся не только к безопасности информации, но и охватывают аспекты кибербезопасности. Поэтому исследования, в частности, должны быть сосредоточены на аспектах управления в вышеуказанных новых областях безопасности информации и кибербезопасности.

В ходе исследований будет продолжаться в полной мере совместная деятельность МСЭ-Т и ОТК1 ИСО/МЭК с целью обеспечить как можно более широкую совместимость решений по обеспечению безопасности. Следует также рассмотреть успех применения решений, разработанных во многих странах как национальные стандарты.

Настоящий Вопрос отличается от Вопросов 2-й Исследовательской комиссии в том, что он посвящен обмену информацией об управлении сетями между сетевыми элементами и системами управления, а также между системами управления в среде TMN. В рамках настоящего Вопроса рассматриваются в первую очередь защита производственных ресурсов, включая информацию и процессы, с целью управления безопасностью информации.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации и Добавления: E.409 (совместно с ИК2), X.1051, X.1052, X.1053, X.1054, X.1055, X.1056, X.1057, X.1058, X.1059, X.1060, X.1061 и Добавления X.Suppl.13, Suppl.27, Suppl.32, Suppl.34 и X.Suppl.36.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.1051rev2.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Каким образом следует определять конкретные вопросы управления безопасностью для организаций электросвязи?

b) Каким образом следует определять управление измерением безопасности в области электросвязи и управлять им?

c) Каким образом следует сопоставлять задачи контроля и средства контроля и интегрировать их с управленческими и эксплуатационными организационными аспектами в организациях электросвязи?

d) Каким образом следует применять концепции и принципы общего управления безопасностью информации, с помощью которых организации могли бы оценивать, направлять, контролировать деятельность, связанную с безопасностью информации, и сообщать о ней в рамках организации?

e) Каким образом следует принимать вариант обработки рисков для управления последствиями инцидента безопасности?

f) Каким образом следует применять передовой опыт, содержащий рекомендации в отношении услуг по обеспечению безопасности, например услуг CDC, включая услуги SOC, MSS и услуги CIRT?

g) Каким образом следует реализовать надлежащее управление безопасностью информации для организаций электросвязи, используя имеющиеся стандарты (МСЭ-T, ИСО/МЭК и т. д.)?

h) Каким образом следует реализовать управление информацией, позволяющей установить личность, и обеспечить его эффективность?

i) Какие необходимо ввести усовершенствования в рассматриваемые существующие Рекомендации или разрабатываемые новые Рекомендации для уменьшения прямого или косвенного воздействия на изменение климата (например, энергосбережение, сокращение выбросов парниковых газов, внедрение систем мониторинга), в секторе электросвязи и ИКТ или других отраслях?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Исследование и разработка структуры для функций управления безопасностью информации, описанных в Рекомендации МСЭ-Т X.1051.

b) Исследование и разработка методики реализации управления безопасностью информации для организаций электросвязи на основе существующих стандартов (МСЭ-T, ИСО/МЭК и т. д.).

c) Исследование и разработка a структуры/руководящих указаний для услуг по обеспечению безопасности, например услуг CDC, включая услуги SOC, MSS и услуги CIRT.

d) Исследование и разработка руководящих указаний по управлению жизненным циклом для средств контроля.

e) Исследование и разработка руководящих указаний по эффективному управлению рисками, например приобретение киберстрахования для обработки рисков.

f) Исследование и разработка руководящих указаний по управлению информацией, позволяющей установить личность.

g) Предложение планов новых Рекомендаций.

h) Оценка итогов вышеупомянутой деятельности с учетом применимости средств и услуг электросвязи.

i) Составление проектов Рекомендаций.

j) Поддержание и ведение, а также усовершенствование Рекомендаций серии X.105x.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 ([Достойная работа и экономический рост](http://www.un.org/development/desa/disabilities/envision2030-goal8.html)),
9 ([Индустриализация, инновации и инфраструктура)](http://www.un.org/development/desa/disabilities/envision2030-goal9.html)

Рекомендации:

Серии X.800, X.1000, X.1100, X.1200 и X.1300

**Вопросы**:

Вопросы МСЭ-Т: 1/17, 2/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17, 15/17 и 14/15

Исследовательские комиссии:

МСЭ-D; МСЭ-R; ИК 2, 9, 11, 13, 15, 16 и 20 МСЭ-Т

Органы по стандартизации:

Азиатско-Тихоокеанская программа по стандартизации (ASTAP); Европейский институт стандартизации электросвязи (ЕТСИ); ПК27 ОТК1 ИСО/МЭК; ПК40 ОТК1 ИСО/МЭК, ТК68 ИСО, ТК215 ИСО; ТК307 ИСО; Национальный институт стандартов и технологий (NIST); Комитет по технологиям электросвязи (TTC); Проект партнерства третьего поколения (3GPP); Форум по реагированию на инциденты и группам безопасности (FIRST)

Вопрос 4/17

Кибербезопасность и противодействие спаму

(Продолжение Вопроса 4/17)

### 1 Обоснование

Ландшафт электросвязи постоянно меняется, а вместе с ним меняются требования к безопасности электросвязи/ИКТ. В этой киберсреде угрозы и атаки в отношении электросвязи/ИКТ постоянно развиваются и становятся все более сложными и адресными, создавая многогранный комплекс проблем для пользователей, поставщиков услуг, операторов и сетей. Существует неотложная потребность в разработке структур и требований безопасности, то есть комплекта Рекомендаций, в том числе отражающих передовой опыт, для того чтобы помочь организациям в управлении рисками кибербезопасности.

Структуры и требования безопасности, направленные на защиту от угроз и атак, включают набор компонентов, который должен охватывать идентификацию, защиту, обнаружение, реагирование и восстановление. Для противодействия атакам с помощью технических средств необходимы комплексные требования, для того чтобы: минимизировать риски, обнаруживать инциденты и оперативно реагировать на них, а также обеспечивать восстановление после их воздействия; обмениваться информацией о кибербезопасности, используя методы обмена информацией о кибербезопасности (CYBEX) и структурированное представление информации об угрозах (STIX); обеспечивать защиту протоколов, инфраструктуры и приложений, которые используются как неотъемлемая часть нашей повседневной связи.

Искусственный интеллект и машинное обучение как никогда ранее широко применяются в различных отраслях и приложениях. Технические средства, основанные на искусственном интеллекте и машинном обучении, должны повышать качество и эффективность технических мер противодействия угрозам и атакам. Внешние услуги по обеспечению безопасности информации (MSS) – это услуги, исполнение которых передано поставщику услуг. Существует два аспекта внешних услуг по обеспечению безопасности информации – технический и управленческий.

Технологии кибербезопасности включают техническую поддержку внешних услуг по обеспечению безопасности информации, обнаружения угроз и реакции на конечных точках, предотвращения/обнаружения вторжения и идентификации источника атак для защиты услуг и персональных данных, включая информацию, позволяющую установить личность (PII), а также обеспечения информационной безопасности (IA) между взаимодействующими объектами.

Обмен информацией о кибербезопасности с использованием методов CYBEX (система обмена информацией о кибербезопасности) и сбора оперативной информации о киберугрозах имеет существенное значение для защиты инфраструктуры электросвязи/ИКТ и для укрепления кибербезопасности в интересах поставщиков электросвязи/ИКТ.

Кроме того, в связи с весьма динамичными темпами эволюции киберугроз необходимо рассматривать технические аспекты, обеспечивающие поддержку процедур, технической политики и структур кибербезопасности. Существует проблема достижения минимального уровня согласования, так как для обеспечения кибербезопасности необходимо сотрудничество между всеми заинтересованными сторонами.

В сфере кибербезопасности широко распространенной проблемой стал спам, влекущей потенциальную потерю доходов поставщиков услуг интернета, операторов электросвязи, операторов подвижной электросвязи и корпоративных пользователей по всему миру. Кроме того, спам создает проблемы для безопасности информационных сетей и сетей электросвязи, так как он используется в качестве средства фишинга и распространения вирусов, "червей", шпионского программного обеспечения, других видов вредоносных программ и т. д. Вследствие этого в принятой ВАСЭ Резолюции 52 соответствующим исследовательским комиссиям было поручено продолжать оказывать поддержку проводимой работе, в частности в 17-й Исследовательской комиссии, касающейся противодействия спаму, и ускорить свою работу по спаму, для того чтобы устранить существующие и будущие угрозы, в рамках круга ведения и специальных знаний МСЭ-Т, в зависимости от случая. Наряду с этим было поручено продолжать сотрудничество с соответствующими организациями, с тем чтобы продолжать разрабатывать в первоочередном порядке технические Рекомендации с целью обмена передовым опытом и распространения информации с помощью проведения совместных семинаров-практикумов, занятий по профессиональной подготовке и т. д. Далее, 17-й Исследовательской комиссии было поручено регулярно представлять Консультативной группе по стандартизации электросвязи отчеты о выполнении этой Резолюции.

Со стремительным ростом мобильного интернета и конвергенцией технологий ИКТ угрозы, которые заключаются в спаме, становятся все более сложными, так как в нем используются новые функции. Основные методы рассылки спама претерпели значительные изменения: от классических форм рекламы и мошенничества до конвергентных вредоносных программ, используемых, в частности, для получения выкупа и осуществления целевых атак. Кроме того, спам нового поколения также является незапрашиваемым и вызывает раздражение потребителей услуг ИКТ, но он наносит даже больший ущерб, чем обычный спам. Целевые атаки часто осуществляются с помощью направленного фишинга – одного из методов социальной инженерии, предназначенного для получения доступа к сетям через законные каналы, такие как электронная почта. Программы-вымогатели – это тип вредоносного программного обеспечения, которое угрожает опубликовать данные о жертве или на постоянной основе заблокировать доступ к этим данным, если не будет заплачен выкуп. Некоторые вредоносные программы, в особенности большинство программ-вымогателей, могут распространяться через вредоносные вложения в сообщениях электронной почты и через зараженные веб-сайты. В связи с развитием технологий искусственного интеллекта/машинного обучения (ИИ/МО), некоторые виды взаимодействия могут инициировать машины, а не люди, в особенности такие как автоматический обзвон, роботизированные чаты, автоматические текстовые сообщения и т. д. Алгоритмы искусственного интеллекта/машинного обучения также могут использовать личную информацию более адресно для поиска целевых получателей, с тем чтобы рассылать огромные объемы коммерческого спама или даже мошеннического спама.

Вследствие широкого развертывания IMT-2020, интернета вещей и других технологий электросвязи/ИКТ спам постепенно начинает затрагивать промышленные системы.

Противодействие спаму было признано глобальной проблемой, требующей всестороннего комплексного подхода. 17-я Исследовательская комиссия, как ведущая исследовательская комиссия по безопасности электросвязи, поддерживающая деятельность по выполнению Резолюции 52 ВАСЭ, имеет все возможности для исследования разнообразных потенциальных технических мер противодействия распространению спама, затрагивающего стабильность и надежность сетей электросвязи. В дополнение к этому, в целях облегчения разработки Рекомендаций создана техническая структура существующих и возможных будущих Рекомендаций по противодействию спаму с помощью технических средств. Наряду с этим для противодействия спаму новых видов следует публиковать новые Рекомендации.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации, Добавления и Технические отчеты: X.1205, X.1206, X.1207, X.1208, X.1209, X.1210, X.1211, X.1212, X.1213, X.1214, X.1215, X.1216, X.1217, X.1218, X.1231, X.1232, X.1233, X.1234, X.1235, X.1240, X.1241, X.1242, X.1243, X.1244, X.1245, X.1246, X.1247, X.1248, X.1249, X.1303, X.1303bis, X.1500, X.1500.1, X.1520, X.1521, X.1524, X.1525, X.1526, X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4, X.1541, X.1542, X.1544, X.1546, X.1550, X.1570, X.1580, X.1581, X.1582 и Добавления X.Suppl.6, X.Suppl.8, X.Suppl.9, X.Suppl.10, X.Suppl.11, X.Suppl.12, X.Suppl.14, X.Suppl.18, X.Suppl.20, X.Suppl.25 и X.Suppl.29, а также Технический отчет TR.usm.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.1246Amd.1, X.1247Amd.1, X.arc‑ev, X.ics-schema X.tsfpp и X.Sup-cs-ml.

### 2 Вопрос

К числу подлежащих изучению вопросов в контексте сетей и систем электросвязи/ИКТ, наряду с прочими, относятся следующие:

a) Каким образом поставщикам услуг электросвязи/ИКТ следует защищать свою инфраструктуру, поддерживать безопасные операции и использовать механизмы гарантии безопасности?

b) Каковы требования безопасности, которые разработчикам и производителям программного обеспечения, протоколов электросвязи, а также систем связи необходимо принимать во внимание при проектировании, разработке и при обмене передовым опытом в киберсреде?

c) Каким образом следует организовать эффективный обмен информацией об уязвимостях, слабых сторонах и способах атак для оказания помощи в процессах, связанных с жизненным циклом уязвимости?

d) Какие необходимы требования и решения, обеспечивающие устойчивость, безопасность и целостность компонуемых систем?

e) Какие необходимы требования и решения в отношении подотчетности, реагирования на инциденты, внешних услуг по обеспечению безопасности, установления авторства атак, а также мониторинга угроз и обмена информацией о рисках в области электросвязи/ИКТ?

f) Какие механизмы необходимы для обмена информацией, относящейся к безопасности и гарантии безопасности, о системах в киберсреде, включая облачные, встраиваемые и компонуемые системы?

g) Каковы возможные способы использования искусственного интеллекта и машинного обучения для оперативного выявления и анализа новых угроз и уязвимостей?

h) Каким образом поставщики электросвязи/ИКТ должны использовать оперативную информацию об угрозах для укрепления своей деятельности по обеспечению безопасности?

i) Каким образом могут использоваться сети для безопасного предоставления важнейших услуг, таких как использование протокола общего оповещения, во время чрезвычайной ситуации национального масштаба?

j) Какие компоненты составляют набор структуры кибербезопасности, который организация может использовать для устранения рисков?

k) Какие руководящие указания и передовой опыт по обеспечению безопасности необходимы для определения, смягчения последствий и уменьшения ущерба от киберугроз, включая вредоносные программные средства, распределенный отказ в обслуживании и социальную инженерию?

l) Какие виды Технических отчетов и Рекомендаций возможно разработать в поддержку процедур, технической политики и структур кибербезопасности?

m) Каким образом различать и выявлять спам?

n) Каковы новые виды спама в существующих и будущих сетях?

o) Каковы опасные последствия распространения спама?

p) Какие технические факторы затрудняют определение источников спама?

q) Каким образом новые технологии, услуги и приложения, такие как мгновенный обмен сообщениями, социальные сети, мобильные приложения, передача голоса на основе технологии долговременного развития (VoLTE) и услуг связи с расширенными возможностями (RCS) и т. д., делают возможным создание и распространение спама?

r) Каким образом возможно определить маршруты, источники и объемы спама для противодействия распространению такого спама и борьбы с ним?

s) Каким образом может быть реализована безопасность пересылки сообщений?

t) Каким образом возможно предотвратить распространение вредоносного программного обеспечения и вредоносных программ по электронной почте?

u) Каким образом возможно определить маршруты, источники и объемы спама, а также оценить объем инвестиций в оборудование и другие технические средства для противодействия такому спаму и борьбы с ним?

v) Каким образом возможно предотвратить целевые атаки с использованием направленного фишинга?

w) Каким образом возможно предотвратить распространение программ-вымогателей по электронной почте?

x) Каким образом возможно выявить и предотвратить спам в форме взаимодействия на основе ИИ/МО?

y) Каким образом обеспечить защиту личной информации после принятия технологии ИИ/МО, для того чтобы не допускать распространения спамовых сообщений?

z) Какая техническая работа уже проводится в рамках IETF, 3GPP, GSMA, M3AAWG, других форумов, а также объединениями частного сектора для решения проблемы спама?

aa) Какая работа по стандартизации сетей электросвязи может потребоваться для эффективного противодействия спаму, затрагивающего стабильность и надежность сети электросвязи?

bb) В чем заключаются действенные и эффективные решения по противодействию спаму?

cc) Каким образом следует разрабатывать общие и конкретные требования для обмена информацией о противодействии спаму?

dd) В чем заключается передовой опыт противодействия спаму?

### 3 Задачи

К числу задач, подлежащих рассмотрению в контексте электросвязи/ИКТ, наряду с прочими, относятся следующие:

a) Сотрудничество в области кибербезопасности с исследовательскими комиссиями МСЭ-Т, ЕТСИ, FIRST, IETF, IEEE, ОТК1 ИСО/МЭК, OASIS, OMA, TCG, 3GPP, 3GPP2 и другими органами по стандартизации.

b) Работа над структурами и Рекомендациями для решения вопроса о том, каким образом поставщики услуг электросвязи/ИКТ могут защитить свою инфраструктуру, поддерживать безопасные операции, а также обмениваться информацией о кибербезопасности.

c) Составление комплекта Рекомендаций для предоставления решений по обеспечению безопасности в отношении подотчетности, гарантии и реагирования на инциденты в области электросвязи/ИКТ.

d) Исследование и определение методов и возможностей обеспечения безопасности для поставщиков услуг с целью координации и обмена информацией об уязвимостях, платформах и кибератаках.

e) Исследование и определение структуры безопасности, состоящей из набора компонентов, который должен охватывать идентификацию, защиту, обнаружение, реагирование и восстановление.

f) Определения способов использования искусственного интеллекта и машинного обучения для оперативного выявления и анализа новых угроз и уязвимостей.

g) Определение способов применения механизмов подотчетности, гарантии и реагирования на инциденты в сетях электросвязи/ИКТ.

h) Разработка руководящих указаний и методов защиты личной информации, а также защиты информации, позволяющей установить личность (PII), с использованием методов CYBEX, STIX и TAXII, а также соответствующих инструментов обеспечения безопасности.

i) Исследование и разработка технических руководящих указаний для поддержки управления угрозами применительно к определению источника кибератак.

j) Предоставление помощи другим исследовательским комиссиям МСЭ-Т в применении соответствующих Рекомендаций по кибербезопасности для конкретных решений по обеспечению безопасности.

k) Разработка примеров передового опыта и руководящих указаний по обмену информацией об уязвимостях и средствах восстановления для оказания помощи в процессах, связанных с жизненным циклом уязвимости.

l) Сотрудничество с другими организациями по разработке стандартов (например, OASIS для включения STIX и TAXII в документы МСЭ).

m) Работа над Рекомендациями и Техническими отчетами по решению проблем кибербезопасности.

n) Функционирование в качестве ведущей группы МСЭ-Т по техническим средствам противодействия спаму, так как спам определен 2-й Исследовательской комиссией.

o) Определение и анализ рисков, связанных с безопасностью сетей электросвязи (на периферии сети и в базовой сети), появление которых обусловлены постоянно изменяющимся характером спама.

p) Определение маршрутов, источников и объема спама, а также оценка объема инвестиций в оборудование и другие технические средства для противодействия такому спаму и борьбы с ним.

q) Разработка всеобъемлющего и актуализированного перечня существующих, используемых и разрабатываемых, технических мер противодействия спаму в сети электросвязи.

r) Разработка новых Рекомендаций по противодействию существующим и появляющимся видам спама.

s) Разработка комплекса технических мер в поддержку безопасности пересылки сообщений.

t) Разработка новых Рекомендаций для предотвращения распространения вредоносного программного обеспечения и вредоносных программ по электронной почте.

u) Разработка комплекса решений для предотвращения целевых атак с использованием направленного фишинга по электронной почте.

v) Разработка новых Рекомендаций для предотвращения распространения программ-вымогателей по электронной почте.

w) Разработка общих и конкретных требований для обмена информацией о противодействии спаму.

x) Определение того, может ли разработка новых Рекомендаций или усовершенствование существующих Рекомендаций, в том числе методов борьбы с рассылкой незапрашиваемых электронных сообщений, вредоносных программ и другого злонамеренного контента, и методов борьбы с использованием дискредитированного сетевого оборудования, включая бот-сети, способствовать усилиям по эффективному противодействию распространению спама, затрагивающего стабильность и надежность сети электросвязи.

y) Разработка комплекса решений или новых рекомендаций для борьбы со спамом в форме взаимодействия на основе ИИ/МО.

z) На регулярной основе представление Консультативной группе по стандартизации электросвязи и Директору Бюро стандартизации электросвязи обновленной информации для ее включения в ежегодный отчет Совету.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 ([Достойная работа и экономический рост](http://www.un.org/development/desa/disabilities/envision2030-goal8.html)),
9 ([Индустриализация, инновации и инфраструктура)](http://www.un.org/development/desa/disabilities/envision2030-goal9.html)

Рекомендации:

Серия X и другие Рекомендации, касающиеся безопасности

Вопросы:

Вопросы МСЭ-Т: 1/17, 2/17, 3/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 и 15/17

Исследовательские комиссии:

ИК 1 и 2 МСЭ-D; ИК 2, 9, 11, 13, 16 и 20 МСЭ-Т

Органы по стандартизации:

Европейский институт стандартизации электросвязи (ЕТСИ); Институт инженеров по электротехнике и радиоэлектронике (IEEE); Целевая группа по инженерным проблемам интернета (IETF); ТК57 МЭК, TК292 МЭК, РГ10 ТК65 МЭК; ПК27 ОТК1 ИСО/МЭК; Национальный институт стандартов и технологий (NIST); Организация по развитию стандартов структурированной информации (OASIS); Открытый альянс подвижной связи (OMA); Открытая группа; Группа управления объектами (OMG); Проект партнерства третьего поколения (3GPP); Второй проект партнерства третьего поколения (3GPP2); Группа по доверенным вычислениям (TCG)

Другие органы:

Рабочая группа по борьбе с фишингом (APWG); Координационный центр групп CERT; группы CIRT; Европейское агентство по безопасности сетей и информации (ENISA); Ассоциация GSM (GSMA); Рабочая группа по борьбе со злоупотреблениями рассылкой сообщений, вредоносным ПО и мобильной связью (M3AAWG); Форум групп реагирования на инциденты и обеспечения безопасности (FIRST); Национальный институт стандартов и технологий (NIST); Организация экономического сотрудничества и развития (ОЭСР)

Вопрос 6/17

Безопасность услуг электросвязи и интернета вещей

(Продолжение Вопроса 6/17)

### 1 Обоснование

В Рекомендации МСЭ‑T X.1101 установлены требования и структура обеспечения безопасности многоадресной передачи. В Рекомендациях МСЭ‑T X.1111, X.1112, X.1113 и X.1114 определена структура безопасности для домашней сети, в том числе профиль сертификата устройства, механизм аутентификации и структура авторизации. В Рекомендациях МСЭ‑T X.1121, X.1122, X.1123, X.1124 и X.1125 содержится всестороннее определение безопасности для сетей подвижной связи. В Рекомендациях МСЭ‑T X.1171, X.1311 и X.1312 представлены структура конфиденциальности для услуг подвижной связи NID, структура безопасности для повсеместной сенсорной сети (USN), руководящие указания по обеспечению безопасности промежуточного программного обеспечения USN и требования безопасности маршрутизации по беспроводным сенсорным сетям, соответственно. В Рекомендациях МСЭ‑T X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197 и X.1198 содержится описание полного набора требований, механизмов и структуры безопасности услуг IPTV. В Добавлениях МСЭ-T X.Suppl.19 и X.Suppl.24 рассматриваются аспекты безопасности эксплуатации мобильных телефонов. В Рекомендациях МСЭ‑T X.1331, X.1332 и Добавлении МСЭ-T X.Suppl.26 описаны аспекты безопасности "умной" электросети. В Рекомендациях МСЭ‑T X.1361, X.1362, X.1363, X.1364 и X.1365 представлены относящиеся к IoT требования, механизмы и структуры безопасности. Необходимо проводить постоянную работу по поддержанию и ведению, а также совершенствованию этих Рекомендаций и Добавлений по вопросам безопасности, с тем чтобы соответствовать потребностям новых технологий и услуг.

Услуги и сети электросвязи и IoT дают возможность каждому получить доступ к любой необходимой информации удобным для пользователя способом, в любое время, в любом месте и с использованием любых устройств. В отрасли электросвязи происходит экспоненциальный рост в сфере услуг электросвязи на основе технологий подвижной связи. В частности, для дальнейшего развития отрасли, сетевых операторов и поставщиков услуг решающее значение имеет безопасность определяемых доменом услуг и сетей электросвязи среди разнородных устройств, в которых используются технологии прикладного уровня, такие как IoT и "умные" города (в том числе межмашинное взаимодействие (M2M), RFID, связь в ближнем поле (NFC) и сенсорная сеть), домашняя сеть, промышленные системы управления (например, "умное" предприятие), "умная" электросеть, встроенный модуль идентификации абонента (eSIM), смартфоны, сеть IPTV и т. д.

Стандартизация оптимальных комплексных решений по обеспечению безопасности имеет важнейшее значение для сетевых операторов и поставщиков услуг, которые работают в международной среде электросвязи с участием многих поставщиков. Ввиду определенных характеристик среды IoT (например, ограниченные вычислительные возможности и ограниченный объем памяти небольших мобильных устройств, длинный жизненный цикл, специализированные операционные системы и программное оборудование), обеспечение безопасности и защита информации, позволяющей установить личность (PII), представляют собой особенно сложную задачу, требующую особого внимания и отдельного исследования.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации и Добавления: X.1101, X.1111, X.1112, X.1113, X.1114, X.1121, X.1122, X.1123, X.1124, X.1125, X.1126, X.1127, X.1171, X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197, X.1198, X.1311, X.1312, X.1313, X.1314, X.1331, X.1332, X.1333, X.1361, X.1362, X.1363, X.1364, X.1365, X.1366, X.1367, X.1368, X.1369, X.1453 и Добавления X.Suppl.19, X.Suppl.24 и X.Suppl.26.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.iotsec-4, X.ra-iot, X.sc-iot, X.ztd-iot и TR.ibc-cd.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Каким образом следует выявлять и определять аспекты безопасности услуг электросвязи и IoT в области подвижной электросвязи?

b) Каким образом следует выявлять и устранять угрозы для услуг электросвязи и IoT?

c) Какие технологии безопасности необходимы для поддержки услуг электросвязи и IoT?

d) Каким образом следует сохранять и поддерживать возможность безопасного присоединения применительно к услугам электросвязи и IoT?

e) Какие образом следует исследовать и разрабатывать технологии обеспечения безопасности, в которых используются технологии на основе ИИ/МО, для услуг электросвязи и IoT?

f) Какие необходимы методы, механизмы и протоколы обеспечения безопасности для новых услуг электросвязи и IoT, в особенности для новых услуг по защите цифрового контента?

g) Каковы глобальные решения по обеспечению безопасности для услуг электросвязи и IoT (например, включая услуги для "умных" городов, "умных" электросетей и ICS (например, "умное" предприятие), базирующихся на сетях электросвязи/ИКТ)?

h) Каковы примеры передового опыта или руководящие указания по безопасным услугам электросвязи и IoT?

i) Какие необходимо ввести усовершенствования в рассматриваемые существующие Рекомендации или разрабатываемые новые Рекомендации для уменьшения прямого или косвенного воздействия на изменение климата (например, энергосбережение, сокращение выбросов парниковых газов, внедрение систем мониторинга), в секторе электросвязи и ИКТ или других отраслях?

j) Какие необходимы механизмы защиты и управления PII (информация, позволяющая установить личность) для безопасных услуг электросвязи и IoT?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Составление комплекта Рекомендаций для предоставления комплексных решений по обеспечению безопасности для безопасных услуг электросвязи и IoT – в сотрудничестве с другими исследовательскими комиссиями МСЭ-Т и организациями по разработке стандартов, в частности IETF, ПК 6, 25, 27, 31 и 41 ОТК1 ИСО/МЭК.

b) Пересмотр существующих Рекомендаций/Стандартов МСЭ-Т, ИСО/МЭК и иных организаций по разработке стандартов в сфере домашних сетей, "умных" электросетей, безопасности смартфонов, IoT и повсеместно распространенных сенсорных сетей с целью определения безопасных услуг электросвязи.

c) Дальнейшее исследование с целью определения аспектов безопасности услуг электросвязи и IoT для среды международной электросвязи с участием многих поставщиков, и для новых услуг (например, "умных" городов, "умных" электросетей и ICS (например, "умное" предприятие), базирующихся на сетях электросвязи/ИКТ).

d) Исследование и определение проблем, связанных с безопасностью и угрозами в безопасных услугах электросвязи и IoT.

e) Исследование и разработка механизмов обеспечения безопасности для безопасных услуг электросвязи и IoT.

f) Исследование и разработка механизмов, обеспечивающих возможность присоединения для безопасных услуг электросвязи и IoT в среде электросвязи с участием одного или многих поставщиков.

g) Исследование и определение проблем защиты и угроз PII для безопасных услуг электросвязи и IoT.

h) Исследование и разработка механизмов защиты и управления PII для безопасных услуг электросвязи и IoT.

i) Исследование и разработка технологий, в которых используются технологии на основе ИИ/МО, для безопасных услуг электросвязи и IoT.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 ([Достойная работа и экономический рост](http://www.un.org/development/desa/disabilities/envision2030-goal8.html)),
9 ([Индустриализация, инновации и инфраструктура)](http://www.un.org/development/desa/disabilities/envision2030-goal9.html),
11 ([Устойчивые города и населенные пункты](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Рекомендации:

Серия X и другие Рекомендации, касающиеся безопасности

Вопросы:

Вопросы МСЭ-Т: 1/17, 2/17, 3/17, 4/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 и 15/17

Исследовательские комиссии:

МСЭ-R; ИК 9, 11, 13, 15, 16 и 20 МСЭ-Т; JCA-IoT и SC&C

Органы по стандартизации:

Целевая группа по инженерным проблемам интернета (IETF); Группа SEG 6 МЭК (микроэлектросети), РГ3 SMB МЭК, ТК 57 и 65 МЭК; ПК 6, 25, 27, 31 и 41 ОТК1 ИСО/МЭК; Открытый альянс подвижной связи (OMA); Проект партнерства третьего поколения (3GPP); Второй проект партнерства третьего поколения (3GPP2)

Другие органы:

Альянс по решениям в отрасли электросвязи (ATIS); Ассоциация по стандартам связи Китая (CCSA); Европейский институт стандартизации электросвязи (ЕТСИ); Ассоциация GSM (GSMA); Альянс M2M; Форум NFC; Национальный институт стандартов и технологий (NIST); oneM2M; Комитет по технологиям электросвязи (TTC); Ассоциация технологий электросвязи (TTA); Форум по архитектуре Universal Plug and Play (UPnP)

Вопрос 7/17

Безопасные прикладные услуги

(Продолжение Вопроса 7/17)

### 1 Обоснование

Рекомендации МСЭ‑T X.1141, X.1142, X.1143, X.1144, X.1145, X.1146, X.1147 составляют комплект Рекомендаций по маркерам безопасности для аутентификации/авторизации и архитектурам безопасности сообщений в сетевых услугах. В Рекомендациях МСЭ‑T X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159 определяются руководящие указания по безопасной аутентификации на основе пароля с обменом ключами и по различным услугам доверенных третьих сторон (TTP). В Рекомендациях МСЭ‑T X.1161, X.1162, X.1163 и X.1164 описана полная структура и механизмы обеспечения безопасности одноранговых (P2P) услуг. Необходимо проводить постоянную работу по поддержанию и ведению, а также совершенствованию этих Рекомендаций по вопросам безопасности, с тем чтобы соответствовать потребностям новых технологий и услуг.

В отрасли электросвязи происходит экспоненциальный рост в сфере услуг доверенных третьих сторон (TTP). Безопасность прикладных услуг на базе электросвязи, включая услуги социальных сетей, P2P, и TTP, имеет решающее значение для дальнейшего развития отрасли. Исключительно важную роль в предоставлении безопасных прикладных услуг играют безопасные протоколы прикладных систем. Стандартизация оптимальных комплексных решений по обеспечению безопасности имеет важнейшее значение для отрасли и сетевых операторов, которые работают в международной среде с участием многих поставщиков. Стандартизации требуется также для исследования и разработки других типов безопасных платформ, прикладных услуг, таких как услуги по проставлению меток времени, безопасные нотариальные услуги, услуги в сфере финансовых технологий (открытый банкинг, пиринговое кредитование, перевод денег, мобильный кошелек, страхование), безопасные услуги OTT (Over The Top) и цифровые двойники; использование подтверждений безопасности вместо сертификатов в протоколах и прикладных услугах на базе инфраструктуры открытых ключей (PKI) и т. д. Технологии безопасности, такие как подтверждение безопасности и подтверждение контроля доступа, становятся критическими в сетях связи.

По мере развития прикладных услуг электросвязи и ИКТ открываются две новые области, которые необходимо исследовать: приложения генерируют и обрабатывают все больше и больше данных, и для поддержки этого теперь требуется искусственный интеллект. Необходимо расширить безопасные прикладные услуги, с тем чтобы охватить обширные исследования и рынок, которые требуются для изучения всего спектра эксплуатационных и технических аспектов защиты данных на основе проводимой работы по услугам анализа данных.

Что касается искусственного интеллекта, поставщики услуг сталкиваются с определенными проблемами в части выбора, подключения и интеграции десятков, если не сотен, компонентов ИИ – с открытым исходным кодом или проприетарных, которые они должны использовать для построения различных решений на основе ИИ (интегрированные приложения, более общие платформы, платформа как услуга и т. д.) в различных инфраструктурах (локальная система, частное облако, гибридное облако, общедоступное облако). Аналогично появлению больших данных, это ставит новые задачи функциональной совместимости в аспекте безопасности, наряду с задачами обеспечения конфиденциальности, целостности и доступности входных данных, используемых ИИ для обучения, и выходных данных, генерируемых ИИ. Все это приводит к возникновению новой поверхности атак ИИ, что требует исследований и разработок. Эта деятельность также может проводиться на основе проводимой работы по услугам анализа данных.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации и Добавления: X.1141, X.1142, X.1143, X.1144, X.1145, X.1146, X.1147, X.1148, X.1149, X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159, X.1161, X.1162, X.1163, X.1164, X.1450, X.1451, X.1452, X.1470 и Добавления X.Suppl.17, X.Suppl.21 и X.Suppl.22.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.1144rev, X.guide-cdd, X.rdda, X.saf-dfs, X.scpa, X.sec-grp-mov, X.sg-dtn, X,sles, X.smdtsc, X.smsrc, X.vide, X.websec-7 и TR.cta.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Каким образом следует выявлять и устранять угрозы для безопасных прикладных услуг?

b) Какие технологии безопасности необходимы для предоставления безопасных прикладных услуг?

c) Каким образом следует сохранять и поддерживать возможность безопасного присоединения применительно к прикладным услугам?

d) Какие методы или протоколы обеспечения безопасности требуются для безопасных прикладных услуг?

e) Какие методы или протоколы обеспечения безопасности требуются для появляющихся безопасных прикладных услуг, включая платформу услуг, услуги в сфере финансовых технологий, услуги OTT?

f) Каковы глобальные решения по обеспечению безопасности для защищенных прикладных услуг и их приложений?

g) Каким образом определить стратегию защиты эксплуатационных и технических данных для прикладных услуг?

h) Каким образом определить стратегию защиты поверхности атак искусственного интеллекта?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Составление всеобъемлющего комплекта Рекомендаций для предоставления комплексных решений по обеспечению безопасности для прикладных услуг связи – в сотрудничестве с другими исследовательскими комиссиями МСЭ-Т и организациями по разработке стандартов, в частности ПК27 ОТК1 ИСО/МЭК.

b) Пересмотр существующих Рекомендаций/Стандартов МСЭ-Т и ИСО/МЭК в области безопасных прикладных услуг.

c) Дальнейшее исследование с целью определения аспектов безопасности применительно к безопасным прикладным услугам и появляющимся новым услугам, таких как услуги в сфере финансовых технологий и услуги ОТТ.

d) Исследование и разработка вопросов безопасности и угроз для безопасных прикладных услуг.

e) Исследование и разработка механизмов обеспечения безопасности для безопасных прикладных услуг.

f) Исследование и разработка стратегий и Рекомендаций по эксплуатационным и техническим аспектам защиты данных для прикладных услуг.

g) Исследование и разработка стратегий и Рекомендаций по защите поверхности атаки искусственного интеллекта.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 ([Достойная работа и экономический рост](http://www.un.org/development/desa/disabilities/envision2030-goal8.html)),
9 ([Индустриализация, инновации и инфраструктура](http://www.un.org/development/desa/disabilities/envision2030-goal9.html)),
11 ([Устойчивые города и населенные пункты](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Рекомендации:

Серия X.800 и другие Рекомендации, касающиеся безопасности

Вопросы:

Вопросы МСЭ-Т: 1/17, 2/17, 3/17, 4/17, 6/17, 8/17, 10/17, 11/17, 14/17, 15/17, 7/13 и 13/17

Исследовательские комиссии:

ИК 2, 9, 11, 13, 16 и 20 МСЭ-Т

Органы по стандартизации:

Целевая группа по инженерным проблемам интернета (IETF); Европейский институт стандартизации электросвязи (ЕТСИ); Ассоциация GSM (GSMA); ПК27 ОТК1 ИСО/МЭК, ПК42 ОТК1 ИСО/МЭК, ТК68 ИСО, ТК307 ИСО; Инициатива Kantara; Организация по развитию стандартов структурированной информации (OASIS); Открытый альянс подвижной связи (OMA); Консорциум World Wide Web (W3C)

Другие органы:

Совет Европы (COE); Европейское агентство по безопасности сетей и информации (ENISA); Альянс Fast Identity Online (FIDO); Международное многостороннее партнерство против киберугроз (ИМПАКТ)

Вопрос 8/17

Безопасность облачных вычислений и инфраструктуры больших данных

(Продолжение Вопроса 8/17)

### 1 Обоснование

Облачные вычисления – это модель, обеспечивающая пользователям услуг возможность повсеместного, удобного сетевого доступа по запросу к совместно используемому набору конфигурируемых вычислительных ресурсов (например, сетей, серверов, системы хранения данных, приложений и услуг), которые могут быть оперативно предоставлены и высвобождены при минимальных управленческих усилиях или минимальном взаимодействии поставщиков услуг. Модель облачных вычислений определяется пятью важнейшими характеристиками (по запросу, предоставление по широкополосной сети доступа, объединение ресурсов, быстрое обеспечение эластичности, самообслуживание и измеряемые услуги); пятью категориями услуг облачных вычислений: программное обеспечение как услуга (SaaS), связь как услуга (CaaS), платформа как услуга (PaaS), инфраструктура как услуга (IaaS) и сеть как услуга (NaaS); а также различными моделями развертывания (государственное, частное, гибридное) и гибким расширением видов предоставления услуг (в центральной, региональной, периферийной области и т. д.). Распространение метода облачных вычислений в качестве предпочтительного средства для обнаружения, выведения на внешний уровень, создания, а также повторного использования услуг в рабочих процессах, приложениях и коммуникационных приложениях придает новое значение необходимости обеспечения безопасности.

Прогнозируемые преимущества облачных вычислений включают гибкое и динамическое предоставление ресурсов, а также упрощенное и автоматизированное администрирование инфраструктуры ИТ. Виртуализация обеспечивает возможность совместного использования практически неограниченных ресурсов, при этом улучшается масштабируемость и существенно сокращаются затраты на управление инфраструктурой. Внедрение периферийных вычислений позволяет осуществлять распределение облачных возможностей на периферию сети. Таким образом возникают реализации облачных услуг, характеризующихся низкой и детерминированной задержкой и высокой надежностью. Однако открытые системы, совместно используемые ресурсы и присущее облачным и периферийным вычислениям межсетевое взаимодействие вызывают многочисленные вопросы обеспечения безопасности, и это, вероятно, является наиболее серьезным барьером, препятствующим признанию облачных вычислений. Перевод в облако подразумевает переход от защищенных традиционных собственных систем ИТ к незащищенным "трансформированным в облако" открытым инфраструктурам. В связи с этим требуется глубокое переосмысление вопросов безопасности.

Облачные вычисления в течение нескольких лет рассматривались как информационная технология, ориентированная на услуги и контролируемая участниками рынка интернета. Тем не менее участники рынка электросвязи должны играть важную роль на развивающемся рынке и в формирующейся экосистеме облачных вычислений. В связи с тем, что облачные услуги предоставляются по сетям электросвязи, участники рынка электросвязи должны обеспечить высокий уровень гарантии. Обеспечение прочной, но гибкой защиты станет одним из ключевых инструментов реализации всего рынка и экосистемы облачных вычислений, в особенности, когда периферийные вычисления обеспечивают более локальное распределение облачных ресурсов. Это обусловливает более сложные взаимосвязи реализаций в периферийных, региональных и центральных областях облака.

Кроме того, гибкое использование обширных ресурсов в среде облачных вычислений обеспечит возможность предоставления новых услуг по обеспечению безопасности, которые не могут быть предоставлены существующими локальными средствами защиты (например, услуги противодействия вредоносному программному обеспечению как облачная услуга).

Большие данные понимаются как технологии, набор инструментов, данные и аналитика, используемые при обработке больших объемов данных. Кроме того, в результате экспоненциального роста данных и превращения их в один из ключевых активов сетей электросвязи/ИКТ, анализ больших наборов данных выполняется с помощью облачных вычислений, для того чтобы выявить закономерности и взаимосвязи, которые в противном случае остались бы скрытыми. Основные процессы больших данных, такие как сбор, хранение, анализ данных, управление ими и их визуализация, осуществляются на основе облачных вычислений, без которых невозможны оперативная передача и анализ больших данных с использованием традиционных технологий (например, большие данные как услуга). Таким образом, необходимо изучить, какие типы мер безопасности могут быть в ближайшем будущем обеспечены с помощью облачных вычислений. Рекомендации МСЭ-T X.1601, X.1602 и X.1631 составляют комплект Рекомендаций по услугам безопасности применительно к обзору, архитектуре и структуре безопасности облачных вычислений, межуровневой безопасности облака, а также конкретным вопросам безопасности сетевых услуг. В настоящее время существует неотложная потребность в обеспечении безопасности важнейших услуг по передаче голоса, мультимедийных услуг, услуг на основе идентичности, услуг гарантии целостности и безопасности информации, услуг определения идентичности и передачи данных, а также экстренных услуг, которые основаны на облачных вычислениях. В рамках настоящего Вопроса предусматривается разработка на основе Части 5 Технического отчета Оперативной группы по облачным вычислениям новых Рекомендаций, по следующим темам:

− передовой опыт и руководящие указания для руководства процессом обеспечения безопасности в среде на базе облачных вычислениях;

− разъяснение сфер ответственности, а также определение требований и угроз безопасности применительно к основным участникам, а также соответствующим ролям в экосистеме облачных вычислений;

− архитектура безопасности, которая основана на эталонной архитектуре, предоставленной в рамках Вопроса 18/13;

− технологии управления безопасностью и аудита безопасности для управления доверием.

В рамках Вопроса 8/17 будет осуществляться совместная деятельность по смежным Вопросам, а именно: 2/17, 3/17, 4/17, 7/17, 10/17 и 11/17, в целях разработки Рекомендаций по безопасности облачных вычислений.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации и Технические отчеты: X.1601, X.1602, X.1603, X.1604, X.1605, X.1606, X.1631, X.1641, X.1642, X.1643, X.1750, X.1751, X.1752 и Технический отчет TR.XAASL.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.BaaS-sec, X.gecds, X.nssa-cc, X.sa-ec, X.sgcnp, X.sgdc, X.sgmc и X.sr-cphr.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Какие следует разработать новые Рекомендации или другие виды документов, предназначенные для основных участников, таких как поставщики услуг, пользователи услуг и партнеры в области услуг, а также других основных заинтересованных сторон отрасли, с тем чтобы повысить безопасность всей экосистемы облачных вычислений, безопасность периферийных вычислений, безопасность сетевого взаимодействия и т. д?

b) Какие следует разработать новые Рекомендации по архитектуре безопасности и организации функциональных возможностей безопасности в соответствии с эталонной архитектурой?

c) Какие следует разработать новые Рекомендации по механизмам гарантирования, технологиям аудита, а также оценке связанных с этим рисков в целях установления доверия между различными участниками?

d) Какие следует разработать новые Рекомендации по решениям безопасности, передовому опыту или руководящим указаниям применительно к платформе больших данных и безопасности инфраструктуры?

e) Какое взаимодействие необходимо обеспечить для сведения к минимуму дублирования деятельности с другими Вопросами, исследовательскими комиссиями и ОРС?

f) Каким образом следует разрабатывать безопасность как услугу для защиты систем электросвязи/ИКТ?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Разработка Рекомендаций и других видов документов, направленных на повышение безопасности облачных вычислений.

b) Разработка Рекомендаций по определению требований и угроз безопасности в целях обеспечения безопасности услуг облачных вычислений на основе общих требований к облачным вычислениям, определенным 13-й Исследовательской комиссией МСЭ-Т.

c) Разработка Рекомендаций по определению архитектуры безопасности и организации функций безопасности на основе эталонной архитектуры, определенной 13‑й Исследовательской комиссией МСЭ-Т.

d) Разработка Рекомендаций по определению надежной, гибкой и эластичной архитектуры безопасностью и ее реализации в системах облачных вычислений.

e) Разработка Рекомендаций по определению механизмов гарантирования, технологий аудита и оценки рисков с целью установления доверительных отношений в рамках экосистемы облачных вычислений.

f) Исследование и разработка Рекомендаций по безопасности платформы и инфраструктуры больших данных, согласованных с эталонной архитектурой, определенной 13‑й Исследовательской комиссией МСЭ-Т.

g) Принятие ответственности за все виды деятельности по безопасности облачных вычислений, а также безопасности платформы и инфраструктуры больших данных в рамках 17‑й Исследовательской комиссии.

h) Представление работы 17-й Исследовательской комиссии, относящейся к безопасности облачных вычислений, в рамках Совместной координационной деятельности по облачным вычислениям.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 ([Достойная работа и экономический рост](http://www.un.org/development/desa/disabilities/envision2030-goal8.html)),
9 ([Индустриализация, инновации и инфраструктура)](http://www.un.org/development/desa/disabilities/envision2030-goal9.html),
11 ([Устойчивые города и населенные пункты](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Рекомендации:

Серия Y по облачным вычислениям

Вопросы:

Вопросы МСЭ-Т: 1/17, 2/17, 3/17, 4/17, 7/17, 10/17, 11/17 и 15/17

Исследовательские комиссии:

ИК 2, 13, 16 и 20 МСЭ-Т

Органы по стандартизации:

Целевая группа по инженерным проблемам интернета (IETF); ПК27 и ПК38 ОТК1 ИСО/МЭК; Организация по развитию стандартов структурированной информации (OASIS) и другие соответствующие определенные органы

Другие органы:

Альянс "За облачную безопасность" (CSA); Целевая группа по распределенному управлению (DMTF)

Вопрос 10/17

Архитектура и механизмы управления определением
идентичности и телебиометрии

(Продолжение Вопроса 10/17)

### 1 Обоснование

Биометрия находит все более широкое применение в приложениях, используемых, в том числе, для проверки идентичности, в таких областях как электронная коммерция, телемедицина и электронное здравоохранение. Прикладные биометрические системы влекут за собой различные проблемы, связанные с защитой операционных и технических данных, надежностью и безопасностью биометрических данных для приложений биометрической безопасности и защищенности.

Биометрическая аутентификация на стороне сервера усложняется и обусловливает более высокие требования, в случае если она осуществляется в открытой сетевой среде. Для приложений электросвязи (таких как телебиометрия), использующих мобильные терминалы и интернет-услуги, требуются методы аутентификации, которые позволят обеспечить высокий уровень безопасности и удобство использования. Необходимо определить требования для безопасного и надежного использования телебиометрических данных при обеспечении усиленной защиты операционных и технических данных.

Управление определение идентичности (IdM) – это управление жизненным циклом и использованием (создание, обслуживание, использование и аннулирование) учетных данных, идентификаторов, атрибутов и шаблонов, по котором объекты (например, поставщики услуг, конечные пользователи, организации, сетевые устройства, приложения и услуги) известны с соответствующим уровнем доверия. В зависимости от контекста для одного элемента возможно существование нескольких идентичностей при различных требованиях к безопасности и в разных местоположениях. В зависимости от модели идентичности контроль над идентичностями может быть централизованным, децентрализованным или сочетанием того и другого. В сетях общего пользования IdM поддерживает безопасный обмен информацией между авторизованными объектами. Это обмен основан на утверждении идентичностей в распределенных системах от нескольких поставщиков услуг. Основой обмена могут также быть различные среды предоставления услуг, например облако и 5G. IdM также способствует укреплению защиты частной информации и, если она базируется на модели доверия, может обеспечить распространение только авторизованной информации.

IdM является ключевым компонентом сетей, услуг и продуктов электросвязи/ИКТ, так как оно помогает установить и поддерживать надежные каналы связи. Наряду с выполнением аутентификации идентичности объекта IdM делает возможным также авторизацию доступа на основе привилегий. IdM также поддерживает изменение привилегий при изменении роли объекта, делегирование и другие услуги на основе идентичности.

IdM – это важнейший компонент управления безопасностью сети, так как оно повышает уровень гарантии для кочевого доступа по запросу к сетям и услугам, которого ожидают конечные пользователи. Наряду с другими механизмами IdM помогает предотвращать мошенничество и кражу идентичности, благодаря чему повышается уверенность пользователей в безопасности и надежности транзакций. В силу лежащего в основе IdM принципа взаимности этот более высокий уровень доверия распространяется как на конечного пользователя, так и на поставщика услуг.

Будут существовать и далее развиваться национальные/региональные конкретные спецификации и решения для IdM. Важно создать фундамент для реализации согласованных решений. В дополнение к исследованию биометрии данный Вопрос посвящен разработке концепции, а также координации и организации всего диапазона деятельности в области IdM в рамках МСЭ-Т. В сотрудничестве с другими исследовательскими комиссиями, другими организациями по разработке стандартов (ОРС) к IdM будет применяться подход "сверху вниз". Следует отметить, что конкретные аспекты IdM (протоколы, требования и идентификаторы сетевых устройств), будут рассматриваться и в рамках других Вопросов.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации и Добавления: X.1080.0, X.1080.1, X.1080.2, X.1081, X.1082, X.1083, X.1084, X.1085, X.1086, X.1087, X.1088, X.1089, X.1090, X.1091, X.1092, X.1093, X.1094, X.1250, X.1251, X.1252, X.1253, X.1254, X.1255, X.1256, X.1257, X.1258, X.1261 (совместно с ИК2), X.1275, X.1276, X.1277, X.1278, X.1279 и Добавления X.Suppl.7 и X.Suppl.35.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.1250rev, X.gpwd, X.oob-sa, X.pet\_auth, X.srdidm и X.tec-idms.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Каким образом осуществлять дальнейшее совершенствование или пересмотр имеющихся Рекомендаций с целью их широкого внедрения и применения?

b) Каковы требования к биометрической аутентификации в сети с широкими функциональными возможностями?

c) Каким образом следует оценивать контрмеры по усилению безопасности для конкретных приложений телебиометрии?

d) Каким образом следует разрабатывать биометрические системы и операции, с тем чтобы они соответствовали требованиям безопасности для любых приложений телебиометрии, включая услуги облачных вычислений?

e) Каким образом возможно усовершенствовать идентификацию и аутентификацию пользователей в части защищенности и безопасности путем применения взаимодействующих моделей в телебиометрии?

f) Какие механизмы необходимо поддерживать для обеспечения защищенных и безопасных операций с биометрическими данными в приложениях телебиометрии – не только существующих, но и появляющихся, например в электронном здравоохранении, телемедицине, электронной коммерции, онлайновых банковских операциях, видеонаблюдении?

g) Каким образом следует разрабатывать биометрические системы и операции, с тем чтобы они соответствовали функциональным требованиям аутентификации объекта для домашних животных с использованием телебиометрии?

h) Каковы функциональные концепции общей инфраструктуры управления определением идентичности (IdM)?

i) Какова надлежащая модель IdM, которая не зависит от сетевых технологий, поддерживает ориентированное на пользователя участие, идентификацию на основе облака, децентрализованные модели идентификации, а также поддерживает безопасный обмен информацией IdM между участвующими объектами (например, пользователями, полагающимися сторонами и поставщиками идентичности) на основе согласия и соответствующих политик?

j) Каковы компоненты общей структуры IdM и требований к IdM?

k) Каковы конкретные требования поставщиков услуг к IdM?

l) Каковы требования, возможности и возможные стратегии обеспечения взаимодействия между различными системами IdM (например, гарантия идентичности, взаимодействие)?

m) Какие вопросы следует рассмотреть для поддержки идентичности в технологиях распределенного реестра, включая кошелек, децентрализованные идентификаторы и проверяемые учетные данные?

n) Каковы возможные механизмы функциональной совместимости IdM, которые включали бы определение и установление применимых профилей с целью минимизации проблем функциональной совместимости?

o) Каковы требования и механизмы для защиты и раскрытия информации, позволяющей установить личность (PII)?

p) Каким образом объект может управлять своими отношениями, когда он участвует в отношениях и взаимодействиях на основе идентичности?

q) Каковы требования к защите систем IdM от кибератак?

r) Какие возможности IdM можно использовать против кибератак?

s) Каким образом IdM должно быть интегрировано в передовые технологии обеспечения безопасности?

t) Каким образом возможно осуществлять аутентификацию без совместных секретных ключей?

u) Возможно ли осуществлять аутентификацию на основе PKI функционально совместимым и безопасным образом?

v) Возможно ли использовать биометрию как часть строгой аутентификации и уровня доверия для обеспечения надежных взаимодействий в сети?

w) Каковы конкретные требования к системе управления определением идентичности на основе потребления в отношении проверки подлинности идентичности и восстановления учетной записи без применения паролей?

x) Каким образом возможно использоваться доверие и отношения для оптимизации восстановления учетной записи, укрепления безопасности пользователей и улучшения пользовательского восприятия при обращении с полагающимися сторонами?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Совершенствование и пересмотр имеющихся Рекомендаций по телебиометрической аутентификации.

b) Рассмотрение сходных элементов и различий между существующими Рекомендациями МСЭ-Т и стандартами ИСО/МЭК по телебиометрии.

c) Исследование и разработка требований и руководящих указаний по безопасности для любого приложения телебиометрии с использованием архитектур и структур, в том числе разработанных в рамках Вопроса 2/17.

d) Исследование и разработка требований для оценки безопасности и методов защиты операционных и технических данных для любого приложения телебиометрии.

e) Исследование и разработка требований к приложениям телебиометрии в сети с широкими функциональными возможностями.

f) Исследование и разработка комплексных структур и требований к приложениям телебиометрии для среды облачных вычислений и хранения данных.

g) Исследование и разработка требований к телебиометрической аутентификации для доверенной структуры идентичности.

h) Исследование и разработка требований к соответствующим общим протоколам, обеспечивающим защищенность, безопасность, защиту операционных и технических данных и получение согласия на "операции с биометрическими данными" в любом приложении телебиометрии, например в области электронного здравоохранения, телемедицины, электронной коммерции, онлайнового банкинга, электронные платежи и видеонаблюдения.

i) Исследование и разработка протоколов биология-машина (B2M) для передачи биологических параметров, совместимых с протоколами межмашинного взаимодействия (M2M).

j) Исследование и разработка приложений телебиометрии с использованием биосигналов для приложений, в том числе, аутентификации, идентификации и мониторинга информации о состоянии здоровья.

k) Исследование и разработка услуг аутентификации объекта для домашних животных с использованием телебиометрии.

l) Описание структуры IdM, которая поддерживает требуемые для IdM обнаружение, модель политики и доверия, аутентификацию и авторизацию, утверждения и управление жизненным циклом учетных данных.

m) Определение функциональных концепций архитектуры IdM, которая включает связывание IdM между сетями и между системами IdM с учетом передовых технологий безопасности.

n) Определение требований (и предложение механизмов) к гарантии идентичности и преобразованию/взаимодействию между различными методами гарантии идентичности, которые могут быть приняты в различных сетях. В таком контексте гарантия идентичности охватывает шаблоны идентичности и репутацию.

o) Определение интерфейсов для функциональной совместимости систем IdM.

p) Определение требований (и предложение механизмов) для защиты и раскрытия информации, позволяющей установить личность (PII).

q) Определение требований (и предложение механизмов) для защиты систем IdM, включая методы использования поставщиками услуг возможностей IdM для координации и обмена информацией о кибератаках.

r) Ведение и координация открытого перечня терминов и определений IdM.

s) Исследование и установление рисков и угроз в области безопасности в сфере IdM.

t) Исследование и разработка децентрализованных систем управления определением идентичности, поддерживающих управление пользователями своей идентичностью.

u) Поддержка доверенных систем управления определением идентичности, которые могут объединяться в федерацию между системами, услугами, устройствами IoT и приложениями.

v) Поддержка системы управления определением идентичности как услуги для агентов облачных услуг, сетей 5G и мобильных устройств.

w) Определение требований и предложение механизмов, обеспечивающих гарантию идентичности для аутентификации и федерации. Определение требований (и предложение механизмов) к гарантии идентичности и установление критериев для преобразования/взаимодействия между различными методами гарантии идентичности, которые могли бы быть приняты в различных сетях. В таком контексте гарантия идентичности охватывает шаблоны идентичности и репутацию.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 ([Достойная работа и экономический рост](http://www.un.org/development/desa/disabilities/envision2030-goal8.html)),
9 ([Индустриализация, инновации и инфраструктура)](http://www.un.org/development/desa/disabilities/envision2030-goal9.html)

Рекомендации:

Серии X и Y

X.200, X.273, X.274, X.509, X.680, X.805 и X.1051

Вопросы:

Вопросы МСЭ-Т: 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 11/17, 15/17, 7/13 и 14/15

Исследовательские комиссии:

ИК1 МСЭ-D; ИК 2/2 МСЭ-D; ИК7 МСЭ-R; ИК 2, 5, 9, 11, 13, 15, 16 и 20 МСЭ-Т

Органы по стандартизации:

ТК25 МЭК, ОРГ1 ТК25 МЭК; Институт инженеров по электротехнике и радиоэлектронике (IEEE); Целевая группа по инженерным проблемам интернета (IETF); ПК 6, 17, 27 и 37 ОТК1 ИСО/МЭК; ТК 12, 68, 215 и 307 ИСО; ОРГ20 ТК12 ИСО, ЕТСИ; OASIS; Инициатива Kantara; 3GPP; 3GPP2

Другие органы:

Международное бюро мер и весов (МБМВ); Международная комиссия по радиологическим единицам и измерениям (МКРЕИ); Альянс Fast Identity Online (FIDO); DID Alliance; Международная организация труда (МОТ); Всемирная организация здравоохранения (ВОЗ)

Вопрос 11/17

Общие технологии (например, Справочник, PKI, формальные языки, идентификаторы объекта) для поддержки безопасные приложения

(Продолжение Вопроса 11/17)

### 1 Обоснование

Данный Вопрос предназначен для поддержки дальнейшего развития различных общих технологий, которые широко используются для поддержки безопасных приложений. К таким технологиям относятся:

− услуги Справочника (серия X.500);

− инфраструктура открытых ключей (PKI – X.509);

− безопасная связь (X.510);

− инфраструктура управления привилегиями (PMI – X.509);

− абстрактная синтаксическая нотация № 1 (ASN.1);

− идентификаторы объекта и органы, осуществляющие их регистрацию;

− нотация для тестирования и управления тестированием версии 3: (TTCN-3);

– поддержка и ведение формальных языков:

• язык спецификации и описания (SDL),

• разработка профиля унифицированного языка моделирования (UML),

• диаграмма последовательности сообщений (MSC),

• нотация требований пользователя (URN),

• CHILL, язык программирования МСЭ-Т;

– поддержка и ведение OSI и ODP.

#### 1.1 Обоснование работы, связанной со Справочниками, PKI и PMI

Рекомендации МСЭ-Т серии X.500 имеют существенное значение для отрасли. Эти Рекомендации посвящены важным компонентам широко применяемых технологий, таких как инфраструктура открытых ключей (PKI) и облегченный протокол доступа к справочнику (LDAP), и используются во многих областях, например финансовой, медицинской и юридической. Там, где требуются услуги Справочника с высоким уровнем безопасности, например в военной области, единственное решение предоставляют Рекомендации серии X.500.

Рекомендации МСЭ-Т серии X.500 обеспечивают тщательно проработанный контроль доступа и защиту конфиденциальности данных. Это открытая спецификация, которая может быть адаптирована ко многим различным приложениям. Предусмотрена возможность расширения, что позволит учесть будущие требования. На приведенной в Рекомендации МСЭ-Т X.500 модели Справочника основан широко используемый LDAP. В Рекомендации МСЭ-Т X.500 описаны возможности взаимодействия с LDAP. Решения для Справочника X.500 и LDAP, являются важной частью управления определением идентичности (IdM).

Рекомендация МСЭ-Т X.509 имеет большое значение. Сертификаты открытых ключей имеют широкое применение.

Наряду с тем, что они играют одну из основных ролей в электронном бизнесе, электронном банкинге, электронном здравоохранении, в настоящее время они используются также в других областях, относящихся к большим сетям с межмашинным взаимодействием и ограниченными объектами, например интернет вещей (IoT) и интеллектуальные электрические сети ("умная" электросеть).

Сертификаты открытых ключей используются также для ряда спецификаций IETF, например для безопасности транспортного уровня (TLS).

Сертификаты атрибутов обеспечивают безопасный метод передачи привилегий, важный для контроля доступа. На сертификатах атрибутов X.509 базируются спецификации языка SAML, разработанного OASIS. Сертификаты атрибутов особенно полезны в случаях, когда привилегии присваивают иные органы, чем те, которые выдают сертификаты открытых ключей.

Необходимо дорабатывать, поддерживать и вести Рекомендацию МСЭ-Т X.509 в сотрудничестве с другими группами, с тем чтобы в ней был отражен и использован опыт, накопленный в области инфраструктуры открытых ключей (PKI) и области инфраструктуры управления привилегиями (PMI). Необходимо совершенствовать Рекомендацию МСЭ-Т X.509, с тем чтобы она соответствовала новым требованиям, таким как связь при межмашинном взаимодействии, безопасность "умных" электросетей, безопасность интернета вещей, квантовые безопасные алгоритмы и технологии распределенного реестра. Разрабатывается децентрализованный механизм PKI на основе блокчейн.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации: Е.104 (совместно с ИК2), Е.115 (совместно с ИК2), F.500, F.510, F.511, F.515, X.500, X.501, X.509, X.510, X.511, X.518, X.519, X.520, X.521, X.525, X.530 и X.1341.

Разрабатываемые Рекомендации по состоянию на 7 января 2022 года: X.510 Amd.1, X.pki-em.

#### 1.2 Обоснование работы, связанной с ASN.1

В случае необходимости будут разработаны дополнительные Рекомендации для учета технологических достижений и дополнительных требований пользователей в отношении нотации ASN.1, ее правил кодирования.

ASN.1 зарекомендовала себя наиболее эффективной нотацией для большого числа групп МСЭ-Т по стандартизации, и многие из них продолжают составлять запросы на исправление сохраняющихся неточностей и неясных мест.

Существует постоянная потребность в предоставлении консультаций и помощи по вопросам, связанным с ASN.1, другим исследовательским комиссиям, внешним организациям по разработке стандартов (ОРС) и странам.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации: X.680, X.681, X.682, X.683, X.690, X.691, X.692, X.693, X.694, X.695, X.696, X.697, X.891, X.892, X.893 и X.894.

Разрабатываемые документы по состоянию на 7 января 2022 года: не имеется.

#### 1.3 Обоснование работы, связанной с идентификаторами объектов и органами их регистрации

Идентификаторы объекта (OID) стали популярной областью имен, которая основана в первую очередь на древовидной иерархической структуре органов регистрации, определяемых целым числом. Их недавнее расширение до международных OID, которые дают возможность идентифицировать дуги с помощью меток Unicode, также пользуется спросом для различных приложений и, возможно, приведет к потребности в дальнейшей разработке и расширении, а также распределении.

Существует постоянная потребность в предоставлении консультаций и помощи другим исследовательским комиссиям, внешним организациям по разработке стандартов (ОРС) и странам по вопросам управления областью имен OID. Ожидается, что с внедрением международных OID и расширением масштабов использования национальных органов регистрации развивающимися странами потребность в помощи и консультациях возрастет. В связи с этим для предоставления таких консультаций и помощи существует постоянная необходимость в "Проекте по OID" МСЭ-Т с назначенным руководителем проекта.

Любое инновационное использование идентификаторов объектов должно разрабатываться совместно со 2-й Исследовательской комиссией МСЭ-Т.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации и Технические документы: X.660, X.662, X.665, X.666, X.667, X.668, X.669, X.670, X.671, X.672, X.674, X.675, X.676, X.677 и Технический документ XSTP-OID-ORS.

Разрабатываемые Рекомендации по состоянию на 7 января 2022 года: X.672rev.

#### 1.4 Обоснование работы, связанной с TTCN-3

Нотация для тестирования и управления тестированием версии 3 (TTCN-3) обеспечивает возможность спецификации тестов функциональных возможностей и функциональной совместимости систем, а также создания общих комплектов тестов. TTCN-3 используется в относящихся к тестированию Рекомендациях МСЭ-Т, разработанных соответствующими ИК МСЭ-Т, в первую очередь ИК11 как ведущей исследовательской комиссией по спецификациям тестирования и проверке на соответствие и функциональную совместимость. МСЭ-T выпускает большое число Рекомендаций. Для обеспечения функциональной совместимости важно, чтобы реализация этих Рекомендаций соответствовала Рекомендациям.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации: X.292, Z.161, Z.161.1, Z.161.2, Z.161.3, Z.161.4, Z.161.5, X.161.6, Z.161.7, Z.162, Z.163, Z.164, Z.165, Z.165.1, Z.166, Z.167, Z.168, Z.169, Z.170 и Z.171.

Разрабатываемые документы по состоянию на 7 января 2022 года: не имеется.

#### 1.5 Обоснование работы, связанной с поддержанием и ведением формальных языков

Не ожидается дальнейшего развития следующих формальных языков:

– язык спецификации и описания (SDL);

– профиль унифицированного языка моделирования (UML);

– диаграмма последовательности сообщений (MSC);

– нотация требований пользователя (URN);

– CHILL, язык программирования МСЭ-Т.

Однако существует необходимость постоянной поддержки и ведения этих языков.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации, Добавления и Руководства пользователя Рекомендацией: Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.110, Z.111, Z.119, Z.120, Z.121, Z.150, Z.151, Z.200, Z.450, а также Добавление Z.Suppl.1 и Руководство пользователя Рекомендацией Z.Imp100.

#### 1.6 Обоснование работы, связанной с поддержанием и ведением OSI

Работа по базовым Рекомендациям, посвященным взаимодействию открытых систем (OSI), завершена. Системы, основанные на Рекомендациях по OSI, могут внедряться в течение относительно длительного периода времени. На основе опыта работы с внедренными системами, базирующимися на этих Рекомендациях, могут быть выявлены технические ошибки или области желательных усовершенствований в этих Рекомендациях. В связи с этим необходимо на постоянной основе осуществлять поддержание и ведение Рекомендации по OSI серии Х.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации и Руководства пользователя Рекомендацией: F.400, F.401, F.410, F.415, F.420, F.421, F.423, F.435, F.440, F.471, F.472, X.200, X.207, X.210, X.211, X.212, X.213, X.214, X.215, X.216, X.217, X.217bis, X.218, X.219, X.220, X.222, X.223, X.224, X.225, X.226, X.227, X.227bis, X.228, X.229, X.233, X.234, X.235, X.236, X.237, X.237bis, X.245, X.246, X.247, X.248, X.249, X.255, X.256, X.257, X.260, X.263, X.264, X.273, X.274, X.281, X.282, X.283, X.284, X.287, X.400, X.402, X.404, X.408, X.411, X.412, X.413, X.419, X.420, X.421, X.435, X.440, X.445, X.446, X.460, X.462, X.467, X.481, X.482, X.483, X.484, X.485, X.486, X.487, X.488, X.610, X.612, X.613, X.614, X.622, X.623, X.625, X.630, X.633, X.634, X.637, X.638, X.639, X.641, X.642, X.650, X.851, X.852, X.853, X.860, X.861, X.862, X.863, X.880, X.881, X.882 и Руководство пользователя Рекомендацией X.ImpOSI.

#### 1.7 Обоснование работы, связанной с поддержанием и ведением ODP

Одним из важнейших аспектов развития систем электросвязи является наличие программного обеспечения, поддерживающего открытую распределенную обработку (ODP). Обеспечение ODP требует стандартизации эталонных моделей, архитектур, функций, интерфейсов и языков (Рекомендации МСЭ-Т серии Х.900).

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации: X.901, X.902, X.903, X.904, X.906, X.910, X.911, X.920, X.930, X.931, X.950, X.952 и X.960.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

#### 2.1 Темы исследования, относящиеся к работе по Справочникам, PKI и PMI

В отношении Справочника:

a) Какие требуются новые определения услуг или изменения в Рекомендациях серии F, для того чтобы определить, каким образом использовать имеющиеся возможности, и каковы новые требования к Рекомендациям X.500?

b) Какие необходимы усовершенствования в Рекомендациях серии E, с тем чтобы они соответствовали новым требованиям к услугам?

c) Какие требуются усовершенствования в Справочнике для поддержки новых требований к PKI?

d) Каковы новые требования к безопасности и конфиденциальности информации Справочника?

e) Какие иные правила кодирования для Рекомендации МСЭ-Т X.500, например XML, могут потребоваться для дальнейшего повышения практической пользы Рекомендации МСЭ-Т X.500?

f) Какие требуются дальнейшие усовершенствования сертификатов открытых ключей и атрибутов, с тем чтобы их можно было использовать в различных средах, например в среде ограниченных ресурсов, межмашинного взаимодействия и крупных сетей?

g) Какие требуются дальнейшие усовершенствования сертификатов открытых ключей и атрибутов, с тем чтобы повысить их практическую пользу в таких областях, как биометрия, аутентификация, управление доступом и электронная коммерция?

h) Какие изменения необходимо внести в Рекомендации МСЭ-T X.509 и МСЭ-T X.510 для поддержки квантовых безопасных алгоритмов и технологий распределенного реестра?

Эта работа будет проводиться в сотрудничестве с ПК6 ОТК1 ИСО/МЭК в рамках ее работы по расширению ИСО/МЭК 9594. Будет поддерживаться сотрудничество с IETF, в особенности в сфере LDAP и PKI.

#### 2.2 Темы исследования, относящиеся к работе по нотации ASN.1

a) Какие требуются усовершенствования в абстрактной синтаксической нотации № 1 (ASN.1) и связанных с ней правилах кодирования для обеспечения потребностей будущих приложений?

b) Какое необходимо сотрудничество, помимо существующих соглашений, с другими органами, занимающимися разработкой де-юре или де-факто стандартов, для обеспечения того, чтобы работа МСЭ-Т в области ASN.1 сохраняла ведущие позиции в сфере разработки нотаций для определения протоколов?

Эта работа будет проводиться в сотрудничестве с ПК6 ОТК1 ИСО/МЭК.

#### 2.3 Темы исследования, относящиеся к работе по идентификаторам объектам и органам их регистрации

a) Какие учебные мероприятия необходимы для поддержки использования OID в различных средах?

b) Какие дополнительные органы регистрации или используемые ими процедуры требуются для поддержки работы по этому и другим Вопросам?

c) Какое необходимо сотрудничество, помимо существующих соглашений, с другими органами, занимающимися разработкой де-юре или де-факто стандартов, для обеспечения того, чтобы работа МСЭ-Т в области OID сохраняла ведущие позиции сфере разработки нотаций для определения протокола и для присваивания однозначных наименований?

Эта работа будет проводиться в сотрудничестве с ПК6 ОТК1 ИСО/МЭК.

#### 2.4 Темы исследования, относящиеся к работе по TTCN

Каким образом необходимо совершенствовать TTCN-3, для того чтобы она отвечала потребностям будущих приложений?

Эта работа будет проводиться в сотрудничестве с ETSI TC MTS.

#### 2.5 Поддержание и ведение формальных языков

Постоянное поддержание и ведение Рекомендаций по SDL, профилю UML, MSC, URN и CHILL.

#### 2.6 Поддержание и ведение OSI

Постоянное поддержание и ведение Рекомендаций по архитектуре OSI и отдельным уровням с целью внесения любых необходимых усовершенствований и исправления любых обнаруженных недостатков. Постоянное поддержание и ведение Рекомендаций по службам и системам обработки сообщений, надежной передаче, дистанционным операциям, CCR и обработке транзакций с целью внесения любых необходимых усовершенствований и исправления любых обнаруженных недостатков.

Для обеспечения как можно более широкого применения разработанных Рекомендаций весьма желательны тесное сотрудничество и взаимодействие с другими исследовательскими комиссиями и другими международными группами, внедряющими OSI.

Эта работа должна проводиться в сотрудничестве с ОТК1 ИСО/МЭК и его подкомитетами.

#### 2.7 Поддержание и ведение ODP

Постоянное поддержание и ведение Рекомендаций по ODP.

Для обеспечения как можно более широкого применения разработанных Рекомендаций весьма желательны тесное сотрудничество и взаимодействие с другими исследовательскими комиссиями и другими международными группами, внедряющими ODP.

Эта работа должна проводиться в сотрудничестве с РГ19 ПК7 ОТК1 ИСО/МЭК.

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

#### 3.1 Задачи в рамках работы по Справочникам, PKI и PMI

a) Ведение и поддержание Справочника путем обработки сообщений об ошибках и включения технических исправлений.

b) Определение новых требований к Справочнику для обеспечения учета новых и существующих технологий.

c) Разработка девятого издания Рекомендаций МСЭ-Т серии X.509.

d) Доработка Рекомендаций МСЭ-T X.509, X.510 и X.pki-em, с тем чтобы они поддерживали новые требования, такие как автоматические процедуры создания и поддержания PKI.

#### 3.2 Задачи в рамках работы по нотации ASN.1

a) Подготовка обновленных Рекомендаций МСЭ-Т серий X.680, X.690 и X.890 в течение исследовательского периода в ответ на потребности пользователей и при необходимости разработка новых изданий.

b) В случае необходимости совершенствования передачи данных, содействие в рамках других Вопросов всех исследовательских комиссий в предоставлении модулей ASN.1, эквивалентных схемам XML, которые определены в Рекомендациях МСЭ-Т (существующих или разрабатываемых), особенно в случае узкой ширины полосы.

c) Мониторинг и оказание помощи в процессе публикации утвержденных Рекомендаций | Международных стандартов и Технических исправлений.

d) Принятие решений по всем отчетам о недостатках и разработка необходимых технических исправлений при необходимости.

e) Обеспечение своевременного и надлежащего рассмотрения всех заявлений о взаимодействии в связи с работой по ASN.1.

f) Разработка любых дополнительных учебных курсов или веб-страниц, которые могут помочь пользователям ASN.1.

#### 3.3 Задачи в рамках работы по идентификаторам объектов и органов их регистрации

a) Подготовка обновленных Рекомендаций МСЭ-Т серий X.660 и X.670 в течение исследовательского периода в ответ на потребности пользователей и при необходимости разработка новых изданий.

b) Мониторинг и оказание помощи в процессе публикации утвержденных Рекомендаций/международных стандартов и технических исправлений.

c) Принятие решений по всем отчетам о недостатках и разработка необходимых технических исправлений, при необходимости.

d) Обеспечение своевременного и надлежащего рассмотрения всех заявлений о взаимодействии в связи с работой по OID.

e) Разработка любых дополнительных учебных курсов или веб-страниц, которые могут помочь пользователям OID.

f) Получение согласия ПК6 ОТК1 ИСО/МЭК и ИК17 на выделение любых дополнительных OID, которые будут сочтены необходимыми.

g) Рассмотрение кандидатов на выполнение функций регистрационных органов по каждому виду имен, охватываемых Рекомендацией МСЭ-T X.660 | ИСО/МЭК 9834-1, предложение ИК17 организации для назначения и информирование ПК 6 ОТК 1 ИСО/МЭК о приглашенном кандидате с помощью заявления о взаимодействии.

h) В рамках сферы ответственности руководителя проекта OID:

• предоставление общих консультаций пользователям OID;

• содействие использованию международных OID в других исследовательских комиссиях и внешних организациях по разработке стандартов (ОРС);

• помощь странам в создании и обеспечении работы национальных органов регистрации для OID (включая международные OID).

#### 3.4 Задачи в рамках работы по TTCN

a) Поддержание и ведение Рекомендаций, относящихся к сфере ответственности настоящего Вопроса.

b) Содействие использованию TTCN в других исследовательских комиссиях и внешних ОРС.

#### 3.5 Задачи в рамках работы по поддержанию и ведению формальных языков

При необходимости, подготовка исправлений или усовершенствований к Рекомендациям по SDL, профилю UML, MSC, URN и CHILL. Поддержание и ведение Руководства пользователя Рекомендацией.

#### 3.6 Задачи в рамках работы по поддержанию и ведению OSI

При необходимости подготовка исправлений или усовершенствований к Рекомендациям по OSI на основе полученных вкладов и исправление любых обнаруженных недостатков. Поддержание и ведение Руководства пользователя Рекомендаций по OSI.

#### 3.7 Задачи в рамках работы по поддержанию и ведению ODP

При необходимости подготовка исправлений или усовершенствований к Рекомендациям по ODP на основе полученных вкладов и исправление любых обнаруженных недостатков.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 ([Достойная работа и экономический рост](http://www.un.org/development/desa/disabilities/envision2030-goal8.html)),
9 ([Индустриализация, инновации и инфраструктура)](http://www.un.org/development/desa/disabilities/envision2030-goal9.html)

Рекомендации:

Серии H.200, H.323, серии H.350, T.120, серии X.600−X.609, серия X.700, серии X.800−X.849, серия Z

Вопросы:

Все Вопросы МСЭ-Т, относящиеся к вышеупомянутым Рекомендациям, и Вопрос 14/17, относящийся к распределенной PKI

Исследовательские комиссии:

ИК 2, 9, 11, 13, 15, 16, 20 МСЭ-Т и все исследовательские комиссии, которые используют Справочник, ASN.1, OID, проверку на соответствие и функциональную совместимость или которым они необходимы

Органы по стандартизации:

Руководящая группа по инженерным проблемам интернета (IESG); Целевая группа по инженерным проблемам интернета (IETF); ТК57 МЭК; ПК 6, 7, 27 и 31 ОТК1 ИСО/МЭК; ТК 68 и 204 ИСО; Организация по развитию стандартов структурированной информации (OASIS); Группа управления объектами (OMG); Консорциум World Wide Web (W3C), Европейский институт стандартизации в области электросвязи (ETSI) TC MTS; ОТК1 ИСО/МЭК и его подкомитеты, которые используют языки проектирования систем МСЭ

Другие органы:

Всемирный почтовый союз (ВПС), Сообщество форума SDL

Вопрос 13/17

Безопасность интеллектуальных транспортных систем

(Продолжение Вопроса 13/17)

### 1 Обоснование

Интеллектуальная транспортная система (ИТС), включая систему автономного вождения, обеспечивает приложения различных типов для повышения безопасности дорожного движения, уменьшения воздействия транспорта на окружающую среду, оптимизации управления дорожным движением и максимального увеличения преимуществ для государственных и коммерческих пользователей.

ИТС охватывают связь различных типов – в транспортных средствах (например, транспортное средства – кочевое устройство), между транспортными средствами (например, транспортное средство – транспортное средства (V2V)) и между транспортными средствами и фиксированными местоположениями (например, транспортное средств – инфраструктура (V2I)), то есть связь транспортного средства с различными объектами (V2X). Для реализации ИТС на автомобильном, железнодорожном, водном и воздушном транспорте, включая навигационные системы, используются информационного-коммуникационные технологии (ИКТ).

Система автоматизированного и ассистированного вождения включает в себя различные компоненты систем, в которых восприятие, принятие решения и управление автомобилем выполнятся не водителем-человеком, но электронными устройствами и машинами, и обеспечивает внедрение автоматизации в дорожном движении.

В среде ИТС, включая системы автоматизированного и ассистированного вождения, уязвимости одного транспортного средства могут передавать в другие транспортные средства, поскольку транспортные средства соединены между собой. Следовательно, необходимо управлять уязвимостями систем связи V2X в транспортном средстве и устранять их, с тем чтобы они не затрагивали большое количество других транспортных средств.

Электронные устройства на борту транспортного средства, такие как электронные управляющие блоки (ECU) и электронные устройства автоматической оплаты проезда (ETC), усложняются. Вследствие этого для повышения производительности и безопасности необходимо надлежащее обновление программных модулей, находящихся в составе этих устройств.

В Рекомендации МСЭ-T X.1373, утвержденной в марте 2017 года, представлена возможность безопасного обновления программного обеспечения для устройств связи в ИТС. В настоящее время осуществляется пересмотр Рекомендации МСЭ-Т X.1373.

Стандартизация оптимальных комплексных решений по обеспечению безопасности имеет важнейшее значение для среды ИТС. Ввиду определенных характеристик связи на борту транспортного средства обеспечение безопасности представляет собой особенно сложную задачу, требующую исследования.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации: X.1371, X.1372, X.1373, X.1374, X.1375, X.1376.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.1373rev, X.edrsec, X.eivnsec, X.evtol-sec, X.fstiscv, X.idse, X.ipscv, X.itssec-5, X.rsu-sec и X.srcd.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Каким образом следует выявлять и определять аспекты безопасности (например, архитектуры и подсистемы безопасности) в среде ИТС и систем автономного и ассистированного вождения?

b) Каким образом следует выявлять и устранять угрозы и уязвимости в услугах и сетях ИТС и систем автономного и ассистированного вождения?

c) Каковы требования безопасности (например, в отношении идентификации и аутентификации) для снижения угроз в среде ИТС и систем автономного и ассистированного вождения?

d) Какие технологии безопасности необходимы для поддержки услуг и сетей ИТС?

e) Каким образом следует сохранять и поддерживать возможность безопасного присоединения между объектами в среде ИТС и систем автономного и ассистированного вождения?

f) Какие необходимы методы, механизмы и протоколы обеспечения безопасности для услуг и сетей ИТС и систем автономного и ассистированного вождения?

g) Каковы согласованные на глобальном уровне решения по обеспечению безопасности для услуг и сетей ИТС и систем автономного и ассистированного вождения, базирующиеся на сетях электросвязи/ИКТ?

h) Каковы примеры передового опыта и руководящие указания по обеспечению безопасности ИТС и систем автономного и ассистированного вождения?

i) Каким образом возможно использовать технологии ИИ/МО для обеспечения безопасности и уверенности при использовании ИТС и системы автономного и ассистированного вождения?

j) Какие механизмы защиты и управления PII (информация, позволяющая установить личность) необходимы для услуг ИТС?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Составление комплекта Рекомендаций для предоставления комплексных решений по обеспечению безопасности для ИТС и системы автономного и ассистированного вождения.

b) Дальнейшее исследование с целью определения аспектов безопасности услуг и сетей ИТС и систем автономного и ассистированного вождения, базирующихся на сетях электросвязи/ИКТ.

c) Исследование и определение проблем и угроз безопасности в ИТС и системе автономного и ассистированного вождения.

d) Исследование и определение требований и сценариев использования для конкретных услуг и приложений ИТС и системы автономного и ассистированного вождения.

e) Исследование и разработка механизмов, протоколов и технологий обеспечения безопасности для ИТС и системы автономного и ассистированного вождения.

f) Исследование и разработка профилирования безопасности, иерархической схемы аутентификации и механизм для конкретных услуг и приложений ИТС и системы автономного и ассистированного вождения.

g) Исследование и разработка приложений алгоритмов эффективного кодирования и декодирования для быстро перемещающихся сетевых узлов и динамически изменяющейся сетевой топологии.

h) Исследование и разработка технологий регистрации данных о событии в контексте ИТС и системы автономного и ассистированного вождения.

i) Исследование и разработка механизмов безопасного присоединения для ИТС и системы автономного и ассистированного вождения в среде электросвязи.

j) Исследование и определение проблем защиты PII и угроз PII в ИТС и системе автономного и ассистированного вождения.

k) Исследование и разработка механизмов защиты и управления PII для ИТС и системы автономного и ассистированного вождения.

l) Исследование и разработка безопасной ИТС и системы автономного и ассистированного вождения на основе технологий ИИ/МО.

m) Исследование и разработка существующих проектов Рекомендации X.1373rev, X.itssec-5, X.srcd, X.edrsec, X.eivnsec, X.fstiscv, X.ipscv, X.rsu-sec, X.evtol-sec.

n) Взаимодействий с соответствующими ОРС с целью совместной разработки Рекомендаций.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 (Достойная работа и экономический рост),
9 (Индустриализация, инновации и инфраструктура),
11 (Устойчивые города и населенные пункты)

Рекомендации:

Серия X и другие Рекомендации, касающиеся безопасности

Вопросы:

Вопросы МСЭ-Т: 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17 и 15/17

Исследовательские комиссии и оперативные группы:

ИК 11, 13, 16 и 20 МСЭ-Т; РГ 5A МСЭ-R; Сотрудничество по стандартам связи для ИТС (CITS); ОГ‑VM (Мультимедиа в автотранспортных средствах) МСЭ-Т

Органы по стандартизации:

ТК 22 и 204 ИСО; ПК 6 и 27 ОТК1 ИСО/МЭК; РГ ИТС IETF; IEEE 802.11 WG и 1609 WG; SAE International (например, Комитет по проектированию систем кибербезопасности транспортных средств, Руководящий комитет по соединенным транспортным средствам, и Комитет по техническим стандартам DSRC); ТК по ITS ЕТСИ; РГ по автомобильным системам W3C

Другие органы:

Ассоциация GSM; ATIS; CCSA; TIA; TTA; TTC; ЕЭК ООН (Экономическая комиссия ООН для Европы): Рабочая группа 29 и вспомогательные органы (например, Целевая группа по кибербезопасности (TFCS)); AGL (Automotive Grade Linux)

Вопрос 14/17

Безопасность технологии распределенного реестра (DLT)

(Продолжение Вопроса 14/17)

### 1 Обоснование

Технологии распределенного реестра (DLT), наиболее известной реализацией которого является блокчейн, представляют собой новый тип безопасных реестров, которые совместно используются, реплицируются и синхронизируются в распределенной среде. Данные в распределенных реестрах управляются несколькими сторонами.

Как особая технология распределенных баз данных, DLT по своей природе устойчива к изменению данных – записанные в блоке, данные невозможно изменить задним числом. Эта важная особенность DLT стала известной после успеха ее первых приложений цифровой криптовалюты, которая называется биткоином.

DLT в настоящее время является одной из революционных технологий, обладающих огромным потенциалом для изменения нашей экономики, культуры и общества. DLT делает возможными инновационные финансовые/нефинансовые децентрализованные приложения, устраняющие потребность во внешних посредниках. На основе DLT будет создана новая инфраструктура управления данными, которая ускорит революционное преобразование услуг в базирующихся на электросвязи отраслях (например, банкинг и финансы, государственное управление, здравоохранение и крупномасштабное материально-техническое обеспечение).

Технологии распределенного реестра окажут огромное влияние на пользователей и сектора электросвязи, включая поставщиков услуг электросвязи.

Необходимо определить функции и обязанности пользователей, операторов и поставщиков услуг электросвязи применительно к аспектам безопасности в среде DLT.

Стандартизация оптимальных комплексных решений по обеспечению безопасности имеет важнейшее значение для DLT, для которой существует большое число сценариев применения в различных секторах, включая отрасль электросвязи. Ввиду определенных характеристик DLT, обеспечение безопасности представляет собой особенно сложную задачу, требующую исследования.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации: X.1400, X.1401, X.1402, X.1403, X.1404, X.1405, X.1406, X.1407 и X.1408.

Разрабатываемые документы по состоянию на 7 января 2022 года: X.sa-dsm, X.sc-dlt, X.srscm-dlt, X.ss-dlt и TR.qs-dlt.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Каким образом следует выявлять и определять в среде DLT аспекты безопасности (например, архитектуры и подсистемы), используя конкретные основы (термины и определения, понятия и таксономия, сценарии использования)?

b) Каким образом следует устранять угрозы и уязвимости в приложениях и услугах на базе DLT?

c) Каковы требования безопасности для снижения угроз в среде DLT?

d) Какие технологии безопасности необходимы для поддержки приложений и услуг на базе DLT?

e) Каким образом следует сохранять и поддерживать возможность безопасного присоединения объектов в среде DLT?

f) Какие необходимы методы, механизмы и протоколы обеспечения безопасности для приложений и услуг на базе DLT?

g) Каковы согласованные на глобальном уровне решения по обеспечению безопасности для приложений и услуг на базе DLT, базирующиеся на сетях электросвязи/ИКТ?

h) Каковы примеры передового опыта и руководящие указания по обеспечению безопасности применительно к приложениям и услугам на базе DLT?

i) Какие механизмы защиты PII (информация, позволяющая установить личность) и управления безопасностью информации необходимы для приложений и услуг на базе DLT?

j) Каким образом возможно использовать DLT для обеспечения безопасности?

k) Каким образом возможно анализировать, оценивать и гарантировать безопасность DLT?

l) С какими заинтересованными сторонами следует сотрудничать ИК17?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Выполнение анализа разрывов в работе по безопасности, которая проводится в других организациях в отношении технологий распределенного реестра.

b) Дальнейшее исследование с целью определения аспектов безопасности приложений и услуг на базе DLT, базирующихся на сетях электросвязи/ИКТ.

c) Исследование основ, таких как термины и определения, понятия и таксономия, сценарии использования, и сценариев использования, относящихся к безопасности, а также к защите PII в сетях DLT.

d) Исследование и определение проблем и угроз безопасности в приложениях и услугах на базе DLT.

e) Исследование и разработка механизмов, протоколов и технологий обеспечения безопасности для приложений и услуг на базе DLT.

f) Исследование и разработка механизмов безопасного присоединения для приложений и услуг на базе DLT.

g) Исследование и определение проблемы защиты PII и угрозы PII в приложениях и услугах на базе DLT.

h) Исследование и разработка системы управления информацией для структур, предоставляющих приложения и услуги на базе DLT.

i) Исследование и разработка руководства по использованию DLT для обеспечения безопасности.

j) Исследование и разработка руководства для осуществления анализа, оценки и гарантии безопасности DLT.

k) Составление комплекта Рекомендаций для предоставления комплексных решений по обеспечению безопасности приложений и услуг на базе DLT.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 (Достойная работа и экономический рост),
9 (Индустриализация, инновации и инфраструктура),
11 (Устойчивые города и населенные пункты)

Рекомендации:

Серия X и другие Рекомендации, касающиеся безопасности

Вопросы:

Вопросы МСЭ-Т: 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17 и 15/17

Исследовательские комиссии:

ИК 5, 11, 13, 16 и 20 МСЭ-Т

Органы по стандартизации:

ТК307 ИСО; ПК27 ОТК1 ИСО/МЭК

Другие органы:

GSMA; W3C; IEEE; ЕЭК ООН (Экономическая комиссия ООН для Европы); FIGI; ATIS; CCSA; TIA; TTA; TTC

Вопрос 15/17

Безопасность для/с помощью появляющихся технологий,
включая квантовую безопасность

(Продолжение Вопроса 15/17)

### 1 Обоснование

ИК17 учитывает динамический характер исследований в области безопасности, которые в существенной степени зависят от гонки потенциалов нападающих и защитников, а также от воздействия инноваций, которые используются обеими сторонами. В результате регулярно появляются новые технологии обеспечения безопасности, и некоторые из них требуют глобальной стандартизации.

Предугадать, что и когда произойдет, невозможно, поэтому ИК17 в инициативном порядке создала и использует механизм инкубации (TP.inno), который обеспечивает управляемую гибкость при исследовании возникающих областей безопасности с целью защиты новых появляющихся услуг и приложений на базе электросвязи/ИКТ.

ИК17, используя этот механизм инкубации, может эффективно определять новые направления работы в появляющихся областях и способствовать разработке ненормативных текстов (Технические документы и Технические отчеты) как подтвержденному передовому опыту, благодаря чему сообщество ИК17 имеет достаточно времени для ознакомления с этими новыми появляющимися областями, а новые участники – для ознакомления с процедурами и средой ИК17 и МСЭ-Т. При разработке новых направлений работы характер появляющейся технологии безопасности иногда свидетельствует о ее близости к существующему Вопросу, и возможна передача этого направления работы для обеспечения максимальной согласованности, эффективности и качества работы ИК17.

Кроме того, этот механизм инкубации позволяет определять тенденции в развитии технологий обеспечения безопасности, которые разрабатываются в рамках данного Вопроса. Ряд возникающих технологий обусловлены следующими факторами:

− сама тема, по сути, находится в стадии возникновения, например квантовая безопасность, безопасные вычисления с участием нескольких сторон, гомоморфизм или теоретически определяемая безопасность для робототехники и т. д.;

− тема не находится в стадии возникновения, но она впервые становится предметом стандартизации, например анализ вредоносных программ, предотвращение потери данных и т. д.;

− разрывы в архитектуре операционной безопасности, которые не относятся к теме ни одного из Вопросов, например сами продукты безопасности; серьезные проблемы интеграции и композиции, свидетельствующие о возникновении новых решений, относящихся к нескольким темам, схем данных безопасности и т. д.

Одна из возникающих областей, определенных в рамках механизма инкубации, – квантовая безопасность. Появление больших квантовых компьютеров порождает вероятность значительных сбоев в работе традиционных систем электросвязи, базирующихся на ИКТ, а также создает существенные риски для безопасности.

Практически, современная криптографическая безопасность основана на сложных в вычислительном отношении задачах: задаче дискретного логарифма и задаче целочисленной факторизации. Считается, что эти задачи сложно решить за приемлемое время, учитывая существующие архитектуры компьютеров, доступных сейчас и в среднесрочной перспективе. Кроме того, криптография с открытым ключом, в которой используются асимметричные ключи, является фундаментом аутентификации в сетях общего пользования. Квантовые компьютеры, по своей природе, могут решать задачи целочисленной факторизации и дискретного логарифма с приемлемой скоростью, поэтому воздействие квантовых компьютеров может разрушить основы, на которых зиждется в настоящее время криптография, угрожая таким образом существованию одной из фундаментальных основ современной киберсреды и цифровизации.

Квантовое распределение ключей (QKD) позволяет двум сторонам создавать общий случайный секретный ключ, известный только им, который может использоваться для шифрования и дешифрования сообщений с использованием традиционных криптографических алгоритмов. QKD присущи два ограничения, и они создают проблемы топологии и интеграции сети: a) это соединение точка-точка (p-t-p) и его возможно использовать только между двумя сторонами – A и B, и b) оно ограничено по расстоянию наземными сетями. С тем чтобы преодолеть эти два ограничения, в отрасли была введена концепция сетей QKD, в состав которых входят 1) ансамбль узлов, которые соединены между собой с помощью систем двухточечного квантового распределения ключей, и 2) система управления, которая используется совместно всеми узлами QKD и встроена в каждый из них. Эта система управления выполняет распределение секретных ключей между двумя и более узлами, которые являются частью одной сети QKD, но необязательно связаны напрямую между собой. В настоящее время коммерческие системы QKD являются достаточно стабильными и зрелыми, поэтому возможно начать планирование крупномасштабных сетей QKD. Компании и организации осуществляют ряд инициатив по развитию сетей QKD, однако не существует общепринятого стандарта, определяющего, что именно представляет собой система QKD.

Кроме того, случайные числа являются одним из фундаментальных элементов системотехники и играют важную роль в криптографии. Случайность, составляющая основу квантовой механики, делает квантовые системы идеальным источником энтропии. Квантовая генерация случайных чисел – одна из самых развитых квантовых технологий, которая обеспечивает множество возможных методов генерации.

Таким образом, квантовая безопасность обеспечивает связь, которая не уязвима для атак со стороны квантовых компьютеров. Для реализации квантовой безопасности необходимы определенные ключевые элементы, в том числе квантовое распределение ключей и квантовый генератор случайных чисел QRNG). Наряду с этим важным условием широкого применения в реальных сетях электросвязи является функциональная совместимость ключевых элементов и функциональных возможностей QKD и QRNG.

Кроме того, существует настоятельная необходимость в исследовании ИК17 квантовой безопасности, устойчивой к квантовым атакам.

В сферу охвата данного Вопроса по состоянию на 7 января 2022 года входят следующие Рекомендации и Технические документы/отчеты: X.1702, X.1710, X.1712, X.1714 и X.1770 и Технические документы/отчеты TP.inno, TP.sgstruct, TR.sec-qkd.

Разрабатываемые документы по состоянию на 7 января 2022 года: Исправление к X.1712, X.icd‑schemas, X.sec\_QKDN\_AA, X.sec\_QKDN\_CM, X.sec\_QKDN\_intrq, X.sec-QKDN-tn, TR.hybsec-qkdn, TR.sec-ai и TR.sgfdm.

### 2 Вопрос

К числу подлежащих изучению вопросов, наряду с прочими, относятся следующие:

a) Каковы новые появляющиеся технологии безопасности?

b) Каковы категории новых появляющихся технологий безопасности?

c) Каковы надежные методы разработки появляющихся технологий безопасности?

d) Какие механизмы являются наиболее эффективными для реализации механизма инкубации?

e) Какие последствия и проблемы для традиционной связи влечет за собой появление крупномасштабных квантовых компьютеров?

f) Какие ключевые элементы необходимы для формирования квантовой безопасности?

g) Какую стратегию перехода следует принять для формирования квантовой безопасности?

h) Каким образом следует устранять угрозы и уязвимости в приложениях квантовой безопасности?

i) Каковы требования безопасности для снижения угроз квантовой безопасности?

j) Какие технологии безопасности необходимы для поддержки квантовой безопасности?

k) Каким образом следует сохранять и поддерживать возможность безопасного присоединения между объектами квантовой безопасности?

l) Какие требования безопасности, методы, механизмы и протоколы обеспечения безопасности необходимы для квантовой безопасности?

m) Каковы согласованные на глобальном уровне решения по обеспечению безопасности для квантовой безопасности, базирующиеся на сетях электросвязи/ИКТ?

n) Каковы примеры передового опыта и руководящие указания по обеспечению безопасности применительно к квантовой безопасности?

### 3 Задачи

К числу задач, наряду с прочими, относятся следующие:

a) Определение новых появляющихся технологий безопасности.

b) Определение новых категорий появляющихся технологий безопасности для завершения разработки стратегии работы по Вопросу M.

c) Возможный перенос новых направлений работы в другой Вопрос, если в ходе их исследования становится более четким соответствие существующему Вопросу.

d) Внедрение механизма инкубации для рассмотрения новых появляющихся областей в ИК17 МСЭ-Т.

e) Составление комплекта технических Рекомендаций для предоставления комплексных решений по обеспечению безопасности при формировании квантовой безопасности.

f) Исследование с целью определения аспектов безопасности квантовой безопасности, базирующихся на инфраструктуре электросвязи/ИКТ.

g) Исследование и определение проблем и угроз безопасности, относящихся к квантовой безопасности.

h) Исследование и разработка требований безопасности, методов, механизмов, протоколов и технологий обеспечения безопасности применительно к квантовой безопасности.

i) Исследование и разработка механизмов безопасного присоединения применительно к квантовой безопасности.

j) Исследование и разработка системы управления информацией для структур, обеспечивающих квантовую безопасность.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК17 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### 4 Относящиеся к Вопросу

Направления деятельности ВВУИО:

C5

Цели в области устойчивого развития:

8 (Достойная работа и экономический рост),
9 (Индустриализация, инновации и инфраструктура),
11 (Устойчивые города и населенные пункты)

Рекомендации:

Серия X и другие Рекомендации, касающиеся безопасности

Вопросы:

Вопросы МСЭ-Т: 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17 и 14/17

Исследовательские комиссии:

ИК 2, 3, 5, 9, 11, 12, 13, 15, 16 и 20 МСЭ-Т

Органы по стандартизации:

TC Cyber, ISG-QKD ЕТСИ; ПК27 ОТК1 ИСО/МЭК; OASIS; IETF

Другие органы:

GSMA; ATIS; CCSA; TIA; TTA; TTC

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