|  |  |  |
| --- | --- | --- |
| itu_logo | **Всемирная ассамблея по стандартизации электросвязи (ВАСЭ-16)Хаммамет, 25 октября – 3 ноября 2016 года** | C:\Users\gaspari\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\logos-02.png |
|  |  |
| **ПЛЕНАРНОЕ ЗАСЕДАНИЕ** | **Документ 20-R** |
|  | **Июнь 2016 года** |
|  | **Оригинал: английский** |
|  |
| 17-я Исследовательская комиссия МСЭ-Т |
| безопасность |
| ОТЧЕТ ИК17 МСЭ-Т ВСЕМИРНОЙ АССАМБЛЕЕ ПО СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ (васэ-16): ЧАСТЬ II – ВОПРОСЫ, ПРЕДЛАГАЕМЫЕ ДЛЯ ИССЛЕДОВАНИЯ В ходе СЛЕДУЮЩЕГО ИССЛЕДОВАТЕЛЬСКОГО ПЕРИОДА (2017–2020 гг.) |
|  |

|  |  |
| --- | --- |
| **Резюме**: | В настоящем вкладе содержатся Вопросы, предлагаемые для исследования в ходе следующего исследовательского периода 2017–2020 годов 17-й Исследовательской комиссии МСЭ-Т для ВАСЭ-16. |

Примечание БСЭ:

Отчет 17-й Исследовательской комиссии для ВАСЭ-16 представлен в следующих документах:

Часть I: **Документ 19** – Общая информация, в том числе предлагаемые изменения в Резолюции 2 ВАСЭ в Приложении 2

Часть II: **Документ 20** – Вопросы, предлагаемые для исследования в ходе следующего исследовательского периода 2017−2020 годов

# 1 Список Вопросов, предлагаемых 17-й Исследовательской комиссией

| Номер Вопроса | Название Вопроса | Статус |
| --- | --- | --- |
| A/17 | Координация деятельности в области безопасности электросвязи/ИКТ | Продолжение Вопроса 1/17 |
| B/17 | Архитектура и структура безопасности | Продолжение Вопроса 2/17 |
| C/17 | Управление безопасностью информации, передаваемой по системам электросвязи | Продолжение Вопроса 3/17 |
| D/17 | Кибербезопасность | Продолжение Вопроса 4/17 |
| E/17 | Противодействие распространению спама техническими средствами | Продолжение Вопроса 5/17 |
| F/17 | Аспекты безопасности услуг и сетей электросвязи | Продолжение Вопроса 6/17 |
| G/17 | Безопасные прикладные услуги | Продолжение Вопроса 7/17 |
| H/17 | Безопасность облачных вычислений | Продолжение Вопроса 8/17 |
| I/17 | Телебиометрия | Продолжение Вопроса 9/17 |
| J/17 | Архитектура и механизмы управления определением идентичности  | Продолжение Вопроса 10/17 |
| K/17 | Общие технологии (справочник, инфраструктура открытых ключей (PKI), инфраструктура управления привилегиями (PMI), абстрактная синтаксическая нотация № 1 (ASN.1), идентификаторы объектов (OID)), поддерживающие безопасные приложения | Продолжение Вопроса 11/17 |
| L/17 | Формальные языки для программного обеспечения систем электросвязи и тестирования | Продолжение Вопроса 12/17 |

# 2 Формулировка Вопросов

проект Вопроса А/17

Координация деятельности в области безопасности электросвязи/ИКТ

(Продолжение Вопроса 1/17)

# 1 Обоснование

Угрозы безопасности инфраструктуры электросвязи и информационно-коммуникационных технологий (ИКТ) увеличиваются – появляются все чаще и становятся все более сложными. Предпринимавшиеся за последние годы усилия по защите инфраструктуры были в некоторой степени раздробленными и направленными на противодействие и до настоящего времени не смогли обеспечить желаемый уровень защиты от угроз. Это затрудняется наличием большого числа организаций, которые работают над различными аспектами безопасности. Такое положение делает координацию и сотрудничество сложными и проблематичными.

Поскольку очень много коммерческих транзакций в мире осуществляется по сетям электросвязи, гарантия безопасности, связанная с использованием соответствующей инфраструктуры киберпространства, имеет огромное значение для бесперебойного функционирования бизнеса, благосостояния граждан и эффективной работы правительств. Атаки червей, вирусов и других злонамеренных кодов затрагивают миллионы компьютеров и сетей электросвязи во всем мире. Экономическое воздействие таких атак огромно. Для борьбы с такими угрозами важнейшее значение имеют интенсивные, постоянные и целенаправленные меры.

Сфера охвата связанных с безопасностью вопросов весьма широка. Понятие безопасности может применяться практически ко всем аспектам электросвязи и информационных технологий. К учету требований безопасности имеются различные подходы. В их число входят:

• Подход "снизу вверх", при котором эксперты разрабатывают меры безопасности для укрепления и защиты отдельной области сети с использованием конкретных контрмер и методов, таких как биометрия и криптография. Хотя этот подход довольно широко используется, он является фрагментарным и нередко приводит к неодинаковому определению и применению мер безопасности.

• Подход "сверху вниз", который представляет собой стратегический путь решения на высоком уровне вопросов безопасности. Для такого подхода требуется знание общего положения дел. Как правило, это более сложный подход, поскольку труднее найти экспертов, которые обладали бы всесторонними познаниями по каждой части сети и ее требованиям к безопасности, чем экспертов с подробными знаниями в одной-двух конкретных областях.

• Сочетание подходов "снизу вверх" и "сверху вниз" при координации, направленной на соединение различных частей. Часто это оказывалось в высшей степени сложным, когда приходилось иметь дело с различными интересами и программами работы.

В предыдущем исследовательском периоде в рамках этого Вопроса было получено много результатов, которые МСЭ-Т считает весьма ценными при пропагандировании своей работы и результатов своей деятельности. К числу примеров относятся "Дорожная карта" по стандартам безопасности, Руководство по безопасности и Сборники материалов по безопасности. В рамках этого Вопроса основное внимание будет по-прежнему уделяться координации и организации всех направлений деятельности по безопасности электросвязи 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). Этот проект направлен на обеспечение более целенаправленных усилий на уровне проектов и стратегическом уровне как в рамках ИК17, так и вне ее.

В своей работе по безопасности ИК17 учитывает Резолюции 7, 11, 40, 50, 52, 58, 64, 65, 67, 70, 73, 75, 76 и 78 ВАСЭ; Резолюции 101, 123, 130, 136, 174, 177, 178, 179, 181; 188, 189, 197, 199, 200 и 201 ПК; и Резолюции 23, 30, 34, 45, 47, 54, 63, 67, 69 и 80 ВКРЭ.

ИК17 также поддерживает Направление деятельности C5 "Укрепление доверия и безопасности при использовании ИКТ" ВВУИО и принятую на Всемирной конференции по развитию электросвязи 2014 года Задачу 3 Дубайского плана действий о повышении доверия и укреплении безопасности при использовании приложений ИКТ.

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 года входят следующие технические отчеты: технический отчет "Безопасность в области электросвязи и информационных технологий".

Разрабатываемые документы: технический отчет об эффективном использовании стандартов безопасности (X.TRsuss).

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

a) Каковы результаты деятельности по данному Вопросу?

b) Какие необходимы 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.), МСЭ необходимо разрабатывать и поддерживать?

d) Какие требуются семинары-практикумы по безопасности и как они могут быть организованы?

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

f) Каковы важнейшие этапы и критерии успеха?

g) Как можно стимулировать интерес Членов Сектора и администраций к работе по обеспечению безопасности и как можно поддерживать полученный импульс?

h) Как можно было бы сделать элементы обеспечения безопасности электросвязи/ИКТ более привлекательными для рынка?

i) Как можно наиболее эффективно донести до правительств и частного сектора информацию об исключительной важности безопасности и неотложной потребности в защите глобальных экономических интересов, которые зависят от наличия прочной и защищенной инфраструктуры электросвязи/ИКТ?

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

# 3 Задачи

Задачи включают, в том числе, следующие:

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

b) Поддерживать и обновлять "Дорожную карту" стандартов безопасности ИКТ.

c) Поддерживать, вести и обновлять Сборники материалов по безопасности МСЭ-Т.

d) Помогать в поддержании и ведении Руководства по безопасности, опубликованного как технический отчет "Безопасность в области электросвязи и информационных технологий", и представить соответствующий вклад в БСЭ.

e) Продолжать разработку технического отчета об эффективном использовании стандартов безопасности.

f) Помогать в определении пробелов в работе по стандартам безопасности электросвязи/ИКТ и содействовать мерам по заполнению таких пробелов.

g) Давать указания по осуществлению стандартов безопасности электросвязи/ИКТ.

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

i) Рассматривать Рекомендации и заявления о взаимодействии от других исследовательских комиссий и ОРС, в соответствующих случаях, для оценки воздействия координации деятельности в области безопасности.

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

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

l) Играть ведущую роль в МСЭ-Т при организации и планировании практикумов и семинаров по вопросам безопасности, в соответствующих случаях.

m) Обеспечивать эффективное и действенное участие в работе по координации деятельности в области безопасности с другими организациями.

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

o) Призывать национальные органы и операторов 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, например в рамках официально созданной ИК17 Региональной группы для Африки.

p) Оказывать помощь ИК17 в преодолении разрыва в стандартизации, выполняя Резолюцию 44 ВАСЭ, Резолюцию 123 ПК и Резолюцию 47 ВКРЭ.

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

# 4 Относящиеся к Вопросу

Рекомендации:

• Серия X и другие Рекомендации, касающиеся безопасности электросвязи/ИКТ

Вопросы:

• Вопросы МСЭ-Т B/17, C/17, D/17, E/17, F/17, G/17, H/17, I/17, J/17, K/17 и L/17

Исследовательские комиссии:

• МСЭ-D, МСЭ-R, ИК 2, 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)

Другие органы:

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

ПРОЕКТ ВопросА b/17

Архитектура и структура безопасности

(Продолжение Вопроса 2/17)

# 1 Обоснование

В Рекомендациях МСЭ-Т X.800, X.802 и X.803 описывается безопасность 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, управление доступом, неотказуемость, конфиденциальность, целостность, а также проверку безопасности и аварийные извещения 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 ОТК1/ПК27 ИСО/МЭК созданы Рекомендации МСЭ-Т X.841, X.842 и X.843 по информационным объектамбезопасностииуслугамдовереннойтретьейстороны.

Требуется дальнейшая работа по поддержанию и ведению, а также совершенствованию этих Рекомендаций по безопасности с целью удовлетворения потребностей появляющихся технологий (например, сети последующих поколений (СПП) ), аспекты безопасности организации сетей с программируемыми параметрами (SDN)/визуализации сетевых функций (NFV), долгосрочное развитие/развитие системной архитектуры (LTE/SAE), руководство по технической реализации систем, обеспечивающих сквозную связь, и сети на базе протокола Интернет) и услуг. Такая работа отражена в Рекомендациях X.1035 и X.1036, в которых приводятся подробные сведения по протоколам обмена аутентифицируемыми с помощью паролей ключами и по распространению и обеспечению выполнения политики.

Вследствие конвергенции и мобильности сети операторов электросвязи и соответствующие информационные системы подвергаются угрозам безопасности новых типов. Нарушители 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 занимается поиском экономически эффективных комплексных решений в области безопасности, которые не зависят от технологии и обеспечивают защиту широкого спектра услуг и приложений. Для обеспечения таких решений в среде, где имеется много поставщиков, сетевая безопасность должна проектироваться 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 и услуг необходимы новые Рекомендации, в которых показывалось бы, как сочетать технологические стандарты и структуры безопасности.

В сферу охвата данного Вопроса по состоянию на 29 апреля 2016 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.1031, X.1032, X.1034, X.1035, X.1036, X.1037 и Добавления X.Suppl.2, X.Suppl.3, X.Suppl.15 и X.Suppl.16 и X.Suppl.23.

Разрабатываемые документы: X.salcm, X.sdnsec-2, X.sgmvno, X.tigsc и X.voLTEsec-1.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

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

b) Какова архитектура всеобъемлющего 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 G/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) Как применяются услуги по обеспечению безопасности для предоставления решений в области безопасности?

k) Как применяется мониторинг инфраструктуры электросвязи/ИКТ для предоставления решений в области безопасности?

# 3 Задачи

Задачи включают, в том числе, следующие:

a) Разработка всеобъемлющего набора 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) Поддержание и ведение, а также усовершенствование Рекомендаций и Добавлений серии X.800 и серии X.103x.

# 4 Относящиеся к Вопросу

Рекомендации:

• Серия X и другие Рекомендации, касающиеся безопасности

Вопросы:

• Вопросы МСЭ-Т A/17, C/17, D/17, E/17, F/17, G/17, H/17, I/17, J/17 и K/17

Исследовательские комиссии:

• ИК2 МСЭ-D, РГ 6B МСЭ-R; ИК 2, 9, 11, 13, 16 и 20 МСЭ-Т

Органы по стандартизации:

• Альянс по решениям в отрасли электросвязи (ATIS); Европейский институт стандартизации электросвязи (ЕТСИ); 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); Второй проект партнерства третьего поколения (3GPP2)

ПРОЕКТ ВопросА С/17

Управление безопасностью информации, передаваемой
по системам электросвязи

(Продолжение Вопроса 3/17)

# 1 Обоснование

Для организаций электросвязи информация и вспомогательные процессы, оборудование электросвязи, сети и средства передачи являются важными производственными ресурсами электросвязи. С тем чтобы организации электросвязи могли должным образом управлять этими производственными ресурсами и правильно продолжать коммерческую деятельность, чрезвычайно большое значение имеет управление безопасностью информации. В связи с этим была разработана Рекомендация МСЭ-Т X.1051, в которой содержатся важные руководящие указания по управлению безопасностью информации для организаций электросвязи.

На основе руководящих указаний по управлению безопасностью информации также были разработаны подробные и конкретные области управления, в том числе управление, структура управления, риски, чрезвычайные происшествия и активы. В связи с Рекомендацией МСЭ-Т X.1051 следует далее изучить новые области. В то же время необходимо поддерживать и обновлять серию Рекомендаций, отражая последние вопросы управления безопасностью информации. Цель состоит в том, чтобы на основе Рекомендации МСЭ-Т X.1051 разработать в МСЭ-Т набор Рекомендаций по управлению безопасностью для электросвязи.

Параллельно с разработкой Рекомендаций по детализированным, конкретным аспектам управления на основе Рекомендации МСЭ-Т X.1051, следует рассмотреть новые сферы электросвязи/ИКТ, требующие принятия новых глобальных контрмер, в том числе облачные вычисления, переход от IPv4 к IPv6 и защиту информации, позволяющей установить личность. Таким образом, следует рассмотреть возможность проведения исследований, в центре внимания которых будут находиться аспекты управления безопасностью в этих новых сферах.

В ходе исследований будут продолжаться в полной мере совместные усилия МСЭ-Т и ОТК1 ИСО/МЭК с целью обеспечить как можно более широкую совместимость решений в области 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 2‑я Исследовательская комиссия занимается вопросами обмена информацией об управлении сетями между сетевыми элементами и системами управления, а также между системами управления в среде сети управления электросвязью (TMN). В рамках настоящего Вопроса рассматриваются в первую очередь защита производственных ресурсов, включая информацию и процессы, с целью управления безопасностью информации.

В сферу охвата настоящего Вопроса по состоянию на 23 марта 2016 года входят следующие Рекомендации и Добавления: E.409 (совместно с ИК2), X.1051, X.1052, X.1054, X.1055, X.1056, Х.1057 и Добавление X.Suppl.13.

Разрабатываемые документы: X.gpim, X.sgsm, X.sup-gisb и X.sup-gpim.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

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

b) Как следует определять конкретные вопросы управления безопасностью для малых и средних организаций электросвязи?

c) Как следует реализовать надлежащее управление безопасностью информации для организаций электросвязи, используя имеющиеся стандарты (МСЭ-T, ИСО/МЭК и др.)?

d) Как следует определить, что такое оценка управления безопасностью информации в электросвязи, и управлять ею?

e) Как следует реализовать надлежащее управление безопасностью информации в среде облачных вычислений?

f) Как следует осуществлять надлежащее управление информацией, позволяющей установить личность?

g) Как следует реализовать управление безопасностью информации в среде IP, включая переход с IPv4 на IPv6?

h) 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), которое оказывают отрасль электросвязи/ИКТ или другие отрасли?

# 3 Задачи

Задачи включают, в том числе, 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 др.).

c) Исследование и разработка руководящих принципов реализации управления безопасностью информации для малых и средних организаций электросвязи (SMTO).

d) Исследование и разработка руководящих принципов управления безопасностью информации для облачных вычислений.

e) Исследование и разработка руководящих принципов или структуры управления безопасностью информации в среде IPv6.

f) Исследование и разработка Рекомендаций по руководящим принципам защиты информации, 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.

# 4 Относящиеся к Вопросу

Рекомендации:

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

Вопросы:

• Вопросы МСЭ-Т A/17, B/17, D/17, E/17, F/17, G/17, H/17, I/17, J/17, K/17 и 14/15

Исследовательские комиссии:

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

Органы по стандартизации:

• Альянс "За облачную безопасность" (CSA), Европейский институт стандартизации электросвязи (ЕТСИ), ПК27 ОТК1 ИСО/МЭК, ТК68 ИСО, ТК215 ИСО, Национальный институт стандартов и технологий (NIST), Комитет по технологиям электросвязи (TTC), Проект партнерства третьего поколения (3GPP)

ПРОЕКТ ВопросА d/17

Кибербезопасность

(Продолжение Вопроса 4/17)

# 1 Обоснование

Положение в области электросвязи постоянно изменяется, а вместе с этим изменяются и соответствующие требования к безопасности электросвязи/ИКТ. В этой киберсреде настоятельно необходимо обеспечить защиту для протоколов, инфраструктуры и приложений, используемых в качестве неотъемлемой части нашего повседневного общения.

Кибербезопасность включает обеспечение безопасности и защиты услуг, личной информации, защиту информации, позволяющей установить личность, и обеспечение сохранности информации (IA) взаимодействующих структур.

Кибератаки по-прежнему широко распространены и причиняют многообразные сложные проблемы пользователям, поставщикам услуг, операторам, а также сетям. Для противодействия кибератакам с помощью технических средств требуется разрабатывать структуры и требования для обнаружения кибератак, защиты от них, смягчения их последствий и восстановления после них, а также обмена информацией по вопросам кибербезопасности.

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 года входят следующие Рекомендации и Добавления: X.1205, X.1206, X.1207, X.1208, X.1209, X.1210, X.1211, 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.1544, X.1546, X.1570, X.1580, X.1581, X.1582 и Добавления X.Suppl.8, X.Suppl.9, X.Suppl.10, X.Suppl.18 и X.Suppl.20.

Разрабатываемые документы: X.1542 (X.simef), X.cogent, X.metric, X.nessa, X.samtn и X.sbb.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

a) Как поставщикам услуг электросвязи/ИКТ следует защищать свою инфраструктуру, поддерживать безопасные операции и использовать механизмы обеспечения безопасности в сетях электросвязи/ИКТ?

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

c) Как следует эффективно обмениваться информацией об уязвимостях для оказания помощи в процессах, связанных с жизненным циклом уязвимости?

d) Какие необходимы требования и решения в отношении обеспечения способности к восстановлению, безопасности и целостности компонуемых систем?

e) Какие необходимы требования и решения в отношении подотчетности, реагирования на инциденты, мониторинга угроз и предупреждения о рисках в области электросвязи/ИКТ?

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

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

h) Какие руководящие указания и примеры передового опыта в области безопасности необходимы для определения, смягчения последствий и уменьшения ущерба от киберугроз, включая вредоносные программные средства, распределенный отказ в обслуживании и "социальную инженерию"?

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), которое оказывают отрасль электросвязи/ИКТ или другие отрасли?

# 3 Задачи

Задачи включают, в том числе, 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, относящимися к возможностям для поставщиков услуг электросвязи/ИКТ защитить свою инфраструктуру, поддерживать безопасные операции и обмениваться информацией по вопросам кибербезопасности.

c) Составление набора Рекомендаций по предоставлению решений по обеспечению безопасности в отношении подотчетности, гарантий и реагирования на инциденты в области электросвязи/ИКТ.

d) Исследование и определение методов и возможностей обеспечения безопасности для поставщиков услуг с целью координации деятельности и обмена информацией, касающейся уязвимостей, платформ, кибератак и пр.

e) Определение методов применения механизмов подотчетности, гарантий и реагирования на инциденты в сетях электросвязи/ИКТ.

f) Разработка руководящих указаний и методов защиты личной информации, а также информации, позволяющей установить личность (PII), с использованием методик CYBEX.

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

h) 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.

# 4 Относящиеся к Вопросу

Рекомендации:

• Серия X и другие Рекомендации, касающиеся безопасности

Вопросы:

• Вопросы МСЭ-Т A/17, B/17, C/17, E/17, F/17, G/17, H/17, I/17, J/17, K/17 и 7/11

Исследовательские комиссии:

• ИК2 (Вопрос 3/2) МСЭ-D, ИК 2, 9, 11, 13 (Вопрос 7/13) и 16 МСЭ-Т

Органы по стандартизации:

• Европейский институт стандартизации электросвязи (ЕТСИ); Институт инженеров по электротехнике и радиоэлектронике (IEEE); Целевая группа по инженерным проблемам интернета (IETF); IEC ТК57, IEC ТК65/WG10; ИСО/МЭК ПК27 ОТК1; 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); Форум групп реагирования на инциденты и обеспечения безопасности (FIRST); Международное многостороннее партнерство против киберугроз (IMPACT); Организация экономического сотрудничества и развития (ОЭСР)

ПРОЕКТ ВопросА E/17

Противодействие распространению спама техническими средствами

(Продолжение Вопроса 5/17)

# 1 Обоснование

Спам стал широко распространенной проблемой, 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 и все чаще используется в качестве средства фишинга и распространения вирусов, "червей", шпионского программного обеспечения, других видов вредоносных программ и т. д. Поэтому в принятой ВАСЭ Резолюции 52 соответствующим исследовательским комиссиям поручалось 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. Кроме того, ей было поручено продолжить 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 поручалось регулярно представлять Консультативной группе по стандартизации электросвязи отчеты о выполнении этой резолюции.

Противодействие распространению спама признано глобальной проблемой, требующей всестороннего комплексного подхода. 17-я Исследовательская комиссия, как ведущая исследовательская комиссия по безопасности электросвязи, поддерживающая деятельность по Резолюции 52 ВАСЭ, весьма подходит для исследования разнообразных возможных технических мер по противодействию 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 распространению спама техническими средствами. Кроме того, следует опубликовать новые Рекомендации по противодействию распространению новых видов спама.

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 года входят следующие Рекомендации и Добавления: X.1231, X.1240, X.1241, X.1242, X.1243, X.1244, X.1245, X.1246, X.1247, и Добавления X.Suppl.6, X.Suppl.11, X.Suppl.12, X.Suppl.14 и X.Suppl.25.

Разрабатываемые документы: X.cspim, X.gcspi, X.tfcma и X.ticsc.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

a) Как понять и определить, что собой представляет спам?

b) Что представляют собой новые виды спама в существующих и будущих сетях?

c) В чем заключаются серьезные последствия распространения спама?

d) Какие технические факторы затрудняют определение источников спама?

e) Как развитие новых технологий, услуг и приложений, таких как мгновенный обмен сообщениями, социальные сети, мобильные приложения, передача голоса с применением технологии долговременного развития (VoLTE)/набора услуг с расширенными возможностями (RCS) и т. д., может открывать возможности для создания и распространения спама?

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

g) Какая необходима работа по стандартизации сетей электросвязи, если она вообще необходима, для эффективного противодействия распространению спама, затрагивающего стабильность и надежность сети электросвязи?

h) В чем заключаются действенные и эффективные решения по противодействию распространению спама?

i) Как разработать общие и конкретные требования для обмена информацией о противодействии спаму?

j) Каковы примеры передового опыта противодействия распространению спама?

# 3 Задачи

Задачи включают, в том числе, следующие:

a) Действовать в качестве ведущей группы МСЭ-Т по техническим средствам противодействия распространению спама, как он описан 2-й Исследовательской комиссией.

b) Определить и проанализировать риски, связанные с безопасностью сетей электросвязи (на периферии сети и в базовой сети), привносимые постоянно изменяющимся характером спама.

c) Разработать всеобъемлющий и актуализированный список используемых или находящихся в процессе разработки ресурсов имеющихся технических мер по противодействию распространению спама в сети электросвязи.

d) Разработать новые Рекомендации по противодействию распространению существующих и появляющихся видов спама.

e) Разработать общие и конкретные требования для обмена информацией о противодействии спаму.

f) Определить, 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.

g) На регулярной основе представлять Консультативной группе по стандартизации электросвязи и Директору Бюро стандартизации электросвязи обновленную информацию с целью ее включения в ежегодный отчет Совету.

# 4 Относящиеся к Вопросу

Рекомендации:

• Серия X

Вопросы:

• Вопросы МСЭ-Т A/17, B/17, C/17, D/17, F/17, G/17, H/17, I/17 и J/17

Исследовательские комиссии:

• ИК1 и ИК2 МСЭ-D, ИК 2, 11, 13 и 16 МСЭ-Т

Органы по стандартизации:

• ОТК1 ИСО/МЭК, Целевая группа по инженерным проблемам интернета (IETF); Европейский институт стандартизации электросвязи (ЕТСИ); Проект партнерства третьего поколения (3GPP); Второй проект партнерства третьего поколения (3GPP2); Открытый альянс подвижной связи (OMA) и другие соответствующие национальные и международные организации по стандартам

Другие органы:

• Ассоциация GSM (GSMA); Рабочая группа по борьбе со злоупотреблениями рассылкой сообщений, вредоностным 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)

ПРОЕКТ ВопросА F/17

Аспекты безопасности услуг и сетей электросвязи

(Продолжение Вопроса 6/17)

# 1 Обоснование

В Рекомендации МСЭ‑T X.1101 устанавливаются требования и структура обеспечения безопасности многоадресной передачи. В Рекомендациях МСЭ‑T X.1111, X.1112, X.1113 и X.1114 описывается структура обеспечения безопасности для домашней сети, включая профиль сертификата устройства, механизм аутентификации и структуру санкционирования. 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 структуры обеспечения конфиденциальности для устройств сопряжения с сетью (NID) в рамках услуг подвижной связи, структуры обеспечения безопасности для повсеместной сенсорной сети (USN), содержатся руководящие указания по обеспечению безопасности промежуточного программного обеспечения USN и требования к 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 обширного комплекса требований, механизмов и структур обеспечения безопасности услуг IPTV. В Добавлениях МСЭ-T X.Suppl.19 и X.Suppl.24 рассматриваются аспекты безопасности эксплуатации мобильных телефонов. Требуется постоянная работа по поддержанию и ведению, а также усовершенствованию этих Рекомендаций и Добавлений по вопросам безопасности, с тем чтобы соответствовать потребностям появляющихся технологий и услуг.

Под услугами и сетями электросвязи понимаются служба, которые дают возможность каждому получить доступ к любой необходимой информации удобным для пользователя способом, в любое время, в любом месте и с использованием любых устройств. Отрасль электросвязи переживает 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 повсеместная сенсорная сеть (в том числе интернет вещей (IoT), межмашинное взаимодействие (M2M), интеллектуальные транспортные системы и сети пятого поколения), домашняя сеть, аспекты безопасности при организации сетей с программируемыми параметрами (SDN)/виртуализации сетевых функций (NFV), "умная" электросеть, сеть подвижной связи (в том числе связь в ближнем поле (NFC), встроенный модуль идентификации абонента (eSIM) и смартфон), сеть многоадресной передачи, сеть IPTV и т. д.

Стандартизация оптимальных всеобъемлющих решений в области безопасности крайне необходима для сетевых операторов и поставщиков услуг, которые работают в среде международной электросвязи с участием многих поставщиков. Ввиду некоторых особых характеристик подвижной электросвязи (например, передача в эфир, ограниченные вычислительные возможности и ограниченный объем памяти небольших мобильных устройств), обеспечение безопасности представляет собой особенно сложную задачу, которая заслуживает особого внимания и отдельного исследования.

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 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.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 и Добавления X.Suppl.19, X.Suppl.24 и X.Suppl.26.

Разрабатываемые документы: X.iotsec-1, X.iotsec-2, X.itsec-1, X.itssec-2, X.msec-9, X.msec-11, X.sdnsec-1, X.sgsec-2 и X.sotavsu.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

a) Как в подвижной электросвязи следует выявлять и определять аспекты безопасности услуг и сетей электросвязи?

b) Как следует выявлять и устранять угрозы для услуг и сетей электросвязи?

c) Каковы технологии безопасности, обеспечивающие поддержку услуг и сетей электросвязи?

d) Как следует сохранять и поддерживать возможность безопасного присоединения между услугами и сетями электросвязи?

e) Какие необходимы методы, механизмы и протоколы обеспечения безопасности для появляющихся услуг и сетей электросвязи, в особенности для появляющихся услуг по защите цифрового контента?

f) Каковы глобальные решения в области безопасности для услуг и сетей электросвязи (например, включая услуги для "умных" электросетей и интеллектуальных транспортных систем, базирующихся на сетях электросвязи/ИКТ)?

g) Каковы примеры передового опыта или руководящие указания для безопасных услуг и сетей электросвязи?

h) 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), которое оказывают отрасль электросвязи/ИКТ или другие отрасли?

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

# 3 Задачи

Задачи включают, в том числе, следующие:

a) В сотрудничестве с другими исследовательскими комиссиями МСЭ-Т и организациями по разработке стандартов, особенно IETF, ПК 6, 25, 27 и 31 ОТК1 ИСО/МЭК, составление набора Рекомендаций для обеспечения комплексных решений в области безопасности для безопасных услуг и сетей электросвязи.

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

c) Дальнейшее изучение с целью определения аспектов безопасности услуг и сетей электросвязи для среды международной электросвязи с участием многих поставщиков, и для появляющихся новых услуг (например, услуг интеллектуальных транспортных систем и "умных" электросетей, базирующихся на сетях электросвязи/ИКТ).

d) Исследование и определение вопросов, связанных с безопасностью и угрозами в безопасных услугах и сетях электросвязи.

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

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

g) Исследование и определение вопросов защиты PII и соответствующих угроз для безопасных услуг и сетей электросвязи.

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

# 4 Относящиеся к Вопросу

Рекомендации:

• Серия X и другие Рекомендации, касающиеся безопасности

Вопросы:

• Вопросы МСЭ-Т A/17, B/17, C/17, D/17, E/17, G/17, H/17, I/17, J/17, K/17, 7/13, 13/16 и 21/16

Исследовательские комиссии:

• МСЭ-R, ИК 9, 11, 13, 15, 16 и 20 МСЭ-Т, JCA-IoT, JCA-IPTV, Сотрудничество по стандартам связи для ИТС (CITS)

Органы по стандартизации:

• Ассоциация GSM (GSMA); Целевая группа по инженерным проблемам интернета (IETF); Группа SEG 6 МЭК (микроэлектросети), РГ3 SMB МЭК, ТК 57 и 65 МЭК, ПК 6, 25, 27 и 31 ОТК1 ИСО/МЭК, ТК204 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) (ТК CYBER, ТК ITS), 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)

ПРОЕКТ ВопросА G/17

Безопасные прикладные услуги

(Продолжение Вопроса 7/17)

# 1 Обоснование

Рекомендации МСЭ‑T X.1141, X.1142, X.1143 и X.1144 составляют набор Рекомендаций по маркерам безопасности для аутентификации/санкционирования и архитектуры 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 определяются всеобъемлющая структура и механизмы обеспечения безопасности одноранговых (P2P) услуг. Требуются постоянные усилия по поддержанию и ведению, а также совершенствованию этих Рекомендаций по безопасности для удовлетворения потребностей появляющихся технологий и услуг.

Отрасль электросвязи переживает 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 всеобъемлющих решений в области безопасности крайне необходима для отрасли и сетевых операторов, которые работают в международной среде с участием многих поставщиков. Она также требуется для исследования и разработки других типов безопасных прикладных услуг, таких, как услуги по проставлению меток времени, защищенные нотариальные услуги, безопасные цифровые финансовые услуги (электронные платежи, электронный банкинг, электронная коммерция), услуги анализа данных и услуги по выявлению вредоносных программных средств и реагированию на них, включая анализ поведения вредоносных программных средств в контролируемых средах, 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 защита управления доступом, приобретают важнейшее значение в сетях связи.

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 года входят следующие Рекомендации и Добавления: X.1141, X.1142, X.1143, X.1144, 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 и Добавления X.Suppl.17, X.Suppl.21 и X.Suppl.22.

Разрабатываемые документы: X.websec-6, X.websec-7 и X.websec-8.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

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

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

c) Как следует поддерживать и развивать возможности безопасного присоединения для прикладных услуг?

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?

f) Каковы глобальные решения в области безопасности для безопасных прикладных услуг и их приложений?

# 3 Задачи

Задачи включают, в том числе, следующие:

a) В сотрудничестве с другими исследовательскими комиссиями МСЭ-Т и организациями по разработке стандартов, особенно с ОТК1/ПК27 ИСО/МЭК, составление всеобъемлющего набора Рекомендаций по обеспечению комплексных решений в области безопасности для прикладных услуг связи.

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

c) Дальнейшее исследование с целью определения касающихся безопасности аспектов безопасных прикладных услуг и появляющихся новых услуг.

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

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

# 4 Относящиеся к Вопросу

Рекомендации:

• Серия X.800 и другие Рекомендации, касающиеся безопасности

Вопросы:

• Вопросы МСЭ-Т A/17, B/17, C/17, D/17, E/17, F/17, H/17, I/17, J/17, K/17, 7/13 и 13/16

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, ТК68 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)

ПРОЕКТ ВопросА H/17

Безопасность облачных вычислений

(Продолжение Вопроса 8/17)

# 1 Обоснование

Облачные вычисления – это модель, которая дает 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 по облачным вычислениям: 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). Распространение метода облачных вычислений в качестве предпочтительного средства для обнаружения, экстернализации, создания и повторного использования услуг в последовательностях операций, приложениях и коммуникационных приложениях придает новое значение необходимости обеспечения безопасности.

Прогнозируемые преимущества облачных вычислений включают гибкое и динамичное предоставление ресурсов и упрощенное автоматизированное администрирование инфраструктуры ИТ. Виртуализация обеспечивает возможность совместного использования практически неограниченных ресурсов, при этом улучшается масштабируемость и существенно сокращаются затраты на управление инфраструктурой. Однако открытые системы и совместно используемые ресурсы облачных вычислений дают основания для многих опасений в отношении безопасности, что, вероятно, является наиболее серьезным барьером, препятствующим признанию облачных вычислений. Перевод в облако подразумевает переход от защищенных традиционных собственных систем ИТ к незащищенным открытым инфраструктурам, "трансформированным в облако". В связи с этим требуется тщательно пересмотреть вопросы безопасности.

В течение нескольких лет облачные вычисления считались информационной технологией, ориентированной на услуги и контролируемой участниками рынка интернета. Тем не менее участникам рынка электросвязи предстоит играть важную роль на появляющемся рынке и в развивающейся экосистеме облачных вычислений. В связи с тем, что облачные услуги предоставляются по сетям электросвязи, участники рынка электросвязи должны обеспечить высокий уровень гарантий. Обеспечение крепкой и гибкой защиты станет одним из ключевых инструментов реализации всего рынка и экосистемы облачных вычислений.

Кроме того, гибкое использование обширных ресурсов в среде облачных вычислений обеспечит возможность предоставления новых услуг в области безопасности, которые не могут быть предоставлены существующими системами защиты в помещениях (например, услуги противодействия вредоносному программному обеспечению как облачные услуги). Таким образом, необходимо изучить вопрос о том, какие меры безопасности могут быть в ближайшем будущем обеспечены с помощью облачных вычислений.

В Рекомендациях МСЭ-T X.1601, X.1602 и X.1631 содержится набор рекомендаций по услугам в области безопасности, касающийся анализа, архитектуры и структуры безопасности облачных вычислений, межуровневой безопасности облачных вычислений, а также конкретных вопросов безопасности сетевых услуг. В настоящее время существует острая необходимость в обеспечении безопасности важнейших услуг по передаче голоса, мультимедийных услуг, услуг на основе идентичности, услуг обеспечения целостности и безопасности информации, услуг определения идентичности и передачи данных, а также услуг связи в чрезвычайных ситуациях, 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:

• передовому опыту и разработке руководящих указаний для руководства процессом обеспечения безопасности в среде, основанной на облачных вычислениях;

• уточнению сфер ответственности, требованиям к безопасности и определению угроз применительно к основным участникам, а также соответствующим ролям в экосистеме облачных вычислений;

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

• технологиям управления безопасностью и аудита безопасности для управления доверием.

В рамках Вопроса Н/17 будет осуществляться совместная деятельность по таким смежным Вопросам, как B/17, C/17, D/17, G/17, J/17 и K/17, в целях разработки Рекомендаций по безопасности облачных вычислений.

В сферу охвата настоящего Вопроса по состоянию на 23 марта 2016 года входят следующие Рекомендации: X.1601, X.1602, X.1631 и X.1642.

Разрабатываемые документы: X.1641 (X.CSCDataSec), X.dsms и X.SRIaaS.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, 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, с тем чтобы повысить безопасность облачных вычислений?

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) Какое взаимодействие необходимо обеспечить для сведения к минимуму дублирования деятельности в рамках других Вопросов, исследовательских комиссий и ОРС?

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

# 3 Задачи

Задачи включают, в том числе, следующие:

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

b) Разработка Рекомендаций по определению требований к безопасности и угроз 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) Принятие ответственности за все виды деятельности по безопасности облачных вычислений в рамках 17‑й Исследовательской комиссии;

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

# 4 Относящиеся к Вопросу

Рекомендации:

• Рекомендации серии Y по облачным вычислениям

Вопросы:

• Вопросы МСЭ-Т А/17, B/17, C/17, D/17, G/17, J/17 и K/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)

ПРОЕКТ ВопросА I/17

Телебиометрия

(Продолжение Вопроса 9/17)

# 1 Обоснование

В течение предыдущего исследовательского периода в рамках Вопроса 9/17 была подготовлена среда для использования биометрии в приложениях электросвязи и разработаны необходимые Рекомендации. Поскольку биометрия широко принята для проверки идентичности в таких приложениях, как электронная коммерция и электронное здравоохранение, в связи с системами биометрических приложений стали появляться различные сложные задачи, связанные с защитой неприкосновенности частной жизни, надежностью и защищенностью биометрических данных для безопасности и защищенности биометрических приложений. Эти задачи становятся еще более сложными и трудными с принятием биометрической аутентификации в открытой сетевой среде.

В настоящее время для приложений электросвязи, в которых используются подвижные терминалы и услуги на базе интернета, требуются методы аутентификации, которые не только обеспечивают высокую степень безопасности, но и удобны пользователям. Примерами таких появляющихся приложений, в которых биометрическая аутентификация будет, как ожидается, соответствовать этим требованиям, являются онлайновые банковские операции с использованием мобильных телефонов и видеонаблюдение с использованием веб-камер или замкнутых телевизионных систем. Таким образом, необходимо указать требования, связанные с использованием Рекомендаций, касающихся безопасности, защищенности и защиты неприкосновенности частной жизни. Кроме того, требуется рассмотреть такие вопросы, как тестирование на соответствие Рекомендациям и функциональную совместимость, а также заполнение базы телебиометрических данных.

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 года входят следующие Рекомендации: X.1080.1, X.1081, X.1082, X.1083, X.1084, X.1086, X.1088, X.1089, X.1090, X.1091 и X.1092.

Разрабатываемые документы: X.bhsm, X.pbact, X.tam, X.th2, X.th3, X.th4, X.th5, X.th6 и X.th13.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

a) Как далее улучшить или пересмотреть имеющиеся Рекомендации с целью их широкого внедрения и применения?

b) Каковы требования к биометрической аутентификации в сети с широкими функциональными возможностями, такой как СПП?

c) Как следует оценивать контрмеры, связанные с безопасностью, для конкретных приложений телебиометрии?

d) Как следует разрабатывать биометрические системы и операции, включая аутентификацию многих факторов, с тем чтобы они соответствовали требованиям в области безопасности для любых приложений телебиометрии, включая услуги облачных вычислений?

e) Как можно усовершенствовать идентификацию и аутентификацию пользователей в отношении защищенности и безопасности за счет 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?

# 3 Задачи

Задачи включают, в том числе, следующие:

a) Совершенствование и пересмотр имеющихся Рекомендаций по телебиометрической аутентификации и заполнение базы телебиометрических данных.

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 в области безопасности для любого приложения телебиометрии с использованием архитектуры и структуры различных видов, в том числе разработанных в рамках Вопроса 2/17.

d) Исследование и разработка требований для оценки безопасности, соответствия и функциональной совместимости с методами защиты неприкосновенности частной жизни 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 телебиометрической архитектуре для среды облачных вычислений и хранения данных.

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

h) Исследование и разработка требований к соответствующим общим протоколам, обеспечивающим защищенность, безопасность, защиту неприкосновенности частной жизни и согласие на "операции с биометрическими данными" в любом приложении телебиометрии, например, электронном здравоохранении, телемедицине, электронной коммерции, онлайновых банковских операциях, электронные платежи и видеонаблюдении.

i) Исследование и разработка протоколов связи биологии с машиной (B2M) для передачи биологических параметров, взаимодействующих с протоколами межмашинной связи (M2M).

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

k) Исследование и разработка протокола голосферической электросвязи.

# 4 Относящиеся к Вопросу

Рекомендации:

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

Вопросы:

• Вопросы МСЭ-Т A/17, B/17, C/17, D/17, E/17, F/17, G/17, H/17, J/17, K/17, 7/13 и 14/15

Исследовательские комиссии:

• ИК 2/2 МСЭ-D, ИК7 МСЭ-R, ИК 2, 5, 9, 11, 13, 15 и 16 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 17, 27 и 37 ОТК1 ИСО/МЭК; ТК 12, 68 и 215 ИСО; ОРГ20 ТК12 МЭК

Другие органы:

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

ПРОЕКТ ВопросА J/17

Архитектура и механизмы управления определением идентичности

(Продолжение Вопроса 10/17)

# 1 Обоснование

Управление определением идентичности (IdM) представляет собой управление жизненным циклом и использованием (созданием, поддержанием, применением, обеспечением и аннулированием) полномочий, идентификаторов, атрибутов, средств аутентификации и удостоверения, и моделей, с помощью которых с определенной степенью уверенности различаются объекты (например, поставщики услуг, конечные пользователи, социальные сети, организации, сетевые устройства, приложения и услуги). В зависимости от контекста может существовать много идентичностей для одного элемента при различных требованиях к безопасности и во многих местоположениях. В облачных сетях и сетях общего пользования IdM делает возможным надежный обмен информацией между авторизованными объектами, который основан на проверке и утверждении идентичностей в распределенных системах. IdM позволяет защитить информацию и обеспечить, чтобы распространялась только санкционированная информация. IdM является ключевым компонентом надлежащего функционирования сетей электросвязи/ИКТ (например, интернета вещей (IoT), облачных и мобильных вычислений, услуг и продуктов), поскольку оно помогает установить и поддерживать надежную связь. Оно не только помогает установить идентичность объекта, но и позволяет санкционировать привилегии, легко изменять привилегии при изменении функций объекта, делегировать полномочия, кочевать и оказывать другие важные услуги, основанные на идентичности.

IdM – это важнейший компонент управления безопасностью сети и обеспечения возможности кочевого доступа по запросу к сетям и электронным услугам, которых сейчас ожидают конечные пользователи. Наряду с другими механизмами защиты IdM помогает предупреждать мошенничество и хищение персональных данных и таким образом увеличивает доверие пользователей к тому, что электронные транзакции являются безопасными и надежными (например, IoT и системы облачных и мобильных вычислений, непосредственно не контролируемые организацией пользователя).

Будут существовать и продолжать развиваться национальные/региональные особые спецификации и решения для IdM. Для глобальной связи большое значение имеет согласование различных национальных/региональных подходов к IdM, спецификаций и вариантов решений в этой области. Для решения этой задачи необходимы стандарты IdM, ориентированные на использование дружественных по отношению к разработчикам сред, способствующие широкомасштабной разработке приложений и инструментария с использованием различных сетевых технологий (т. е. HTTP, JSON, OAUTH и OpenID Connect).

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) и консорциумами к IdM будет применяться подход "сверху вниз". Признается, 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 23 марта 2016 года входят следующие Рекомендации и Добавления: X.1250, X.1251, X.1252, X.1253, X.1254, X.1255, X.1256, X.1257, X.1275, и Добавление X.Suppl.7.

Разрабатываемые документы: X.1258 (X.eaaa) и X.te.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

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

b) Какова надлежащая модель IdM, независимая от сетевых технологий, обеспечивающая участие, ориентированное на пользователя, предоставляющая связанную с IdM информацию и помогающая осуществлять надежный обмен информацией о IdM между участвующими объектами (например, пользователями, зависимыми сторонами и поставщиками идентичности)?

c) Какие компоненты необходимы для объединения социальных, мобильных и корпоративных моделей IdM таким образом, чтобы содействовать повышению безопасности цифровых транзакций?

d) Каковы функциональные аспекты моделей IdM?

e) Каковы конкретные требования поставщиков услуг и потребителей услуг к IdM?

f) Каковы атрибуты идентичности, которые могут использоваться совместно поставщиками идентичности в доверенной среде?

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

h) Каковы подходящие механизмы для возможности взаимодействия в рамках IdM, которые включали бы определение и установление применимых профилей с целью сведения к минимуму проблем, связанных с возможностью взаимодействия?

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

j) Каковы требования к защите систем IdM от кибератак?

k) Какие возможности IdM можно использовать против кибератак?

l) Каким образом IdM должно быть включено в усовершенствованные технологии обеспечения безопасности?

m) Какие особые требования к IdM связаны с облачными вычислениями?

n) Какие особые требования к IdM связаны с мобильными вычислениями?

o) Какие уникальные требования к IdM связаны с различными распределенными средами, такими как IoT и облако?

p) Каким образом возможно интегрировать проверку подлинности идентичности в системы IdM?

q) Каким образом возможно интегрировать защищенное управление полномочиями в системы IdM?

r) Каким образом возможно интегрировать технологии аутентификации в системы IdM?

# 3 Задачи

Задачи включают, в том числе, следующие:

a) Определение структуры IdM, которая обеспечивала бы требуемые для IdM в эволюционирующей среде представление информации, модель политики и обеспечения надежности, аутентификацию и авторизацию, утверждение и управление жизненным циклом полномочий.

b) Установление функциональных концепций архитектуры IdM, которая включала бы соединение, относящееся к IdM, между сетями и среди систем IdM с учетом усовершенствованных технологий обеспечения безопасности.

c) 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 включает определение моделей и репутации.

d) Предложение руководящих принципов функциональной совместимости систем IdM.

e) Определение требований (и предложение механизмов) для защиты систем IdM, включая пути использования возможностей IdM как способов координации деятельности между поставщиками услуг и обмена между ними информацией, касающейся кибератак.

f) Ведение и координация терминологии и открытого списка определений IdM, и продолжение текущей работы.

g) Исследование и определение рисков и угроз в области безопасности в сфере IdM.

# 4 Относящиеся к Вопросу

Рекомендации:

• Серии X и Y

Вопросы:

• Вопросы МСЭ-Т A/17, C/17, D/17, F/17, G/17 и H/17

Исследовательские комиссии:

• ИК1 и ИК2 МСЭ-D, ИК 2, 3, 11, 13,16 и 20 МСЭ-Т, КГСЭ

Органы по стандартизации:

• Целевая группа по инженерным проблемам интернета (IETF); Европейский институт стандартизации электросвязи (ЕТСИ), ПК 6, 27 и 37 ОТК1 ИСО/МЭК

Другие органы:

• Национальный институт стандартов и технологий (NIST); Организация по развитию стандартов структурированной информации (OASIS); Проект партнерства третьего поколения (3GPP); Второй проект партнерства третьего поколения (3GPP2)

ПРОЕКТ ВопросА K/17

Общие технологии (такие как Справочник, PKI, ASN.1, идентификаторы объекта), поддерживающие безопасные приложения

(Продолжение Вопроса 11/17)

# 1 Обоснование

Данный Вопрос имеет целью содействие продолжению разработки ряда широко используемых общих технологий, поддерживающих безопасные приложения. К ним, в частности, относятся:

• Справочные службы (серия X.500);

• Инфраструктура открытых ключей (PKI – X.509);

• Инфраструктура управления полномочиями (PMI – X.509);

• Нотация ASN.1 (серии X.680 и X.690), идентификаторы объекта и органы, осуществляющие их регистрацию (серии X.660 и X.670);

• Быстрые веб-сервисы и Быстрый информационный набор (серия X.890);

• Поддержание и ведение OSI и ODP.

## 1.1 Обоснование работы в области справочных служб, PKI и PMI

Рекомендации МСЭ-Т серии X.500 оказывают существенное воздействие на отрасль. Эти Рекомендации являются важными компонентами широко применяемых технологий, таких как инфраструктура открытых ключей (PKI) и облегченный протокол доступа к справочникам (LDAP), и используются во многих областях, например финансовой, медицинской и юридической. Там, где требуются справочные службы с высокой степенью защиты, например в военной области, единственное решение обеспечивают Рекомендации серии X.500.

В Рекомендациях МСЭ-Т серии X.500 предусмотрена тщательно проработанная система контроля доступа и защиты неприкосновенности частных данных. Это открытая спецификация, которая может быть адаптирована ко множеству различных приложений. В ней предусмотрена возможность расширения, что позволит учесть будущие требования. На представленной в Рекомендации МСЭ-Т X.500 модели справочника основан широко используемый LDAP. В Рекомендации МСЭ-Т X.500 предусмотрены возможности взаимодействия с LDAP. Содержащиеся в Рекомендации МСЭ-Т X.500 и LDAP решения, касающиеся справочников, являются важной частью управления определением идентичности (IdM). Поставщики справочников предлагают на рынке варианты справочников как системы IdM. Некоторые требования, связанные с IdM и СПП (например, для приложений на основе тегов), могут быть удовлетворены с использованием справочной службы.

Рекомендация МСЭ-Т X.509 имеет большое значение. Сертификаты открытых ключей широко используются. В каждой защищенной сессии браузера, где используется протокол защиты транспортного уровня (TLS), применяется сертификат для аутентификации веб-сервера и согласования ключа шифрования, который будет использоваться для защиты информации, обмениваемой в ходе сессии. Сертификат открытого ключа также используется для аутентификации и защиты электронной почты. На Рекомендации МСЭ-Т X.509 базируется работа Рабочей группы PKIX IETF, CA/браузерного форума, рабочей группы ETSI по электронным подписям и инфраструктуре (ESI), и т. д.

Сертификаты атрибутов обеспечивают защищенный метод передачи привилегий, особенно в системах интегрированного управления определением идентичности. На сертификатах атрибутов, описанных в Рекомендации МСЭ-Т X.509, основываются спецификации разработанного OASIS языка SAML. Сертификаты атрибутов особенно полезны в случаях, когда привилегии присваиваются не теми органами, которые выдают сертификаты открытых ключей, и когда необходимы долгосрочные и отзывные привилегии, например в случае участия объектов в группах.

Рекомендации МСЭ-Т серии X.500 необходимо дорабатывать, с тем чтобы они соответствовали будущим требованиям к IdM, СПП и связи в ближнем поле.

Рекомендацию МСЭ-Т X.509 необходимо дорабатывать, поддерживать и вести в сотрудничестве с другими комиссиями, с тем чтобы она отражала и использовала опыт, накопленный в сферах инфраструктуры открытых ключей (PKI) и инфраструктуры управления полномочиями (PMI). Рекомендацию МСЭ-Т X.509 необходимо совершенствовать, с тем чтобы она соответствовала новым требованиям, таким как связь при межмашинном взаимодействии, безопасность "умных" электросетей и безопасность интернета вещей.

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 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.511, X.518, X.519, X.520, X.521, X.525 и X.1341.

Разрабатываемые Рекомендации: X.pki-em (Инфраструктура открытого ключа: создание и сопровождение) и X.pki-prof (Инфраструктура открытого ключа: профиль).

## 1.2 Обоснование работы, касающейся нотации ASN.1, идентификаторов объекта и органов, осуществляющих их регистрацию

В случае необходимости будут разработаны дополнительные Рекомендации для учета технического прогресса и дополнительных требований пользователей нотации ASN.1, ее правил кодирования, а также дополнительных требований пользователей и поставщиков из регистрационных органов к международным идентификаторам объекта.

Как оказалось, ASN.1 является предпочитаемой нотацией для большого числа групп МСЭ-Т по стандартизации, многие из которых продолжают составлять запросы на исправление остающихся неточностей и неясных мест в более поздних добавлениях и изменениях к этим Рекомендациям.

Оказалось, что идентификаторы объекта (OID) – это весьма распространенная область имен, основанная в первую очередь на древовидной иерархической структуре органов регистрации, определяемая целыми значениями. Их последнее 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 в создании приложений.

Имеется постоянная потребность в предоставлении консультаций и помощи другим исследовательским комиссиям, внешним организациям по разработке стандартов (ОРС) и странам как по вопросам, связанным с нотацией ASN.1, так и – во все большей степени – по управлению областью имен OID. Ожидается, что с внедрением международных OID и расширением масштабов использования национальных регистрационных органов развивающимися странами потребность в помощи и консультациях увеличится. В связи с этим для предоставления таких консультаций и помощи существует 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 23 марта 2016 года входят следующие Рекомендации: 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.680, X.681, X.682, X.683, X.690, X.691, X.692, X.693, X.694, X.695, X.696, X.891, X.892 и X.893.

Разрабатываемые Рекомендации: X.894 (X.cms), X.jsoner, X.oid-iot (Руководящие указания по использованию идентификаторов объектов для интернета вещей), X.oiddev (Информационная технология – Использование идентификаторов объектов для идентификации устройств в интернете вещей) и X.cms (Синтаксис криптографических сообщений).

## 1.3 Обоснование работы по поддержанию и ведению OSI

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 обнаружены технические ошибки, либо выявлена желательность усовершенствований в этих Рекомендациях. В связи с этим необходимо продолжать поддерживать и вести Рекомендации по OSI серии Х.

Работа по базовым Рекомендациям по взаимодействию открытых систем (OSI) завершена.

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 года входят следующие Рекомендации: 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 и X.882.

Разрабатываемые документы: не имеется.

## 1.4 Обоснование работы по поддержанию и ведению ODP

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

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 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

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

## 2.1 Темы исследования, относящиеся к работе в области справочных служб, PKI и PMI

По отношению к справочным службам:

a) Какие требуются новые определения служб или изменения в Рекомендациях серии F, для того чтобы определить, каким образом можно 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 справочника для поддержки новых требований к PKI?

d) Какие имеются новые требования к безопасности и конфиденциальности справочной информации?

e) Какие иные правила кодирования для Рекомендации МСЭ-Т X.500, например XML, могут потребоваться для дальнейшего повышения полезности 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 ресурсы, межмашинного взаимодействия и крупных сетей?

g) Какие требуются дальнейшие усовершенствования сертификатов открытых ключей и атрибутов, с тем чтобы они были более полезными в таких областях, как биометрия, аутентификация, управление доступом и электронная коммерция?

h) Какие изменения требуются внести в Рекомендацию МСЭ-Т X.509, для того чтобы определить усовершенствования и исправить недостатки?

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

## 2.2 Темы исследования, относящиеся к нотации ASN.1, идентификаторам объекта и органам регистрации

a) Какие требуются усовершенствования в абстрактной синтаксической нотации версии 1 (ASN.1) и связанных с ней правилах кодирования для обеспечения потребностей будущих приложений?

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

c) Какие дополнительные регистрационные органы или используемые ими процедуры требуются для обеспечения работы по этому и другим Вопросам?

d) 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 и OID оставалась ведущей в сфере разработки нотаций для определения протокола и для присваивания однозначных наименований?

## 2.3 Темы исследования, относящиеся к работе по поддержанию и ведению OSI

a) Постоянное поддержание и ведение Рекомендаций по архитектуре OSI и отдельным уровням с целью внесения любых необходимых усовершенствований и исправления любых отмеченных недостатков; и

b) 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 отмеченных недостатков.

Для обеспечения как можно более широкого применения полученных в результате 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.

## 2.4 Темы исследования, относящиеся к работе по поддержанию и ведению ODP

Продолжать поддержание и ведение Рекомендаций по ODP.

Для обеспечения как можно более широкого применения полученных в результате 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

Задачи включают, в том числе, следующие:

## 3.1 Задачи, относящиеся к работе в области справочных служб, PKI и PMI

a) Ведение справочника путем учета сообщений об ошибках и включения технических исправлений.

b) Определение новых требований к справочнику для обеспечения учета новых и имеющихся технологий.

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

d) Доработка Рекомендаций МСЭ-T X.509, X.pki-prof и X.pki-em, с тем чтобы они поддерживали новые требования.

## 3.2 Задачи, относящиеся к работе, касающейся нотации ASN.1, идентификаторов объекта и органов, осуществляющих их регистрацию

a) Мониторинг и учет публикаций по всем работам, которые велись на время завершения предыдущего исследовательского периода.

b) Сотрудничество с ОТК1/ПК6 ИСО/МЭК по вопросам, представляющим взаимный интерес.

c) Подготовка обновленных Рекомендаций МСЭ-Т серий X.660, X.670, X.680 X.690 и X.890 в течение данного исследовательского периода в ответ на потребности пользователей и при необходимости разработки новых изданий.

d) В случае необходимости усовершенствовать передачу данных, оказывать 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 небольшой ширины полосы.

e) Вести мониторинг и оказывать помощь в процессе публикации утвержденных Рекомендаций | Международных стандартов и технических исправлений.

f) Принимать решения по всем отчетам о недостатках, имеющимся по состоянию на начало данного исследовательского периода (а также по любым новым отчетам, которые могут быть представлены в течение этого исследовательского периода), и обеспечивать разработку необходимых технических исправлений.

g) Обеспечить своевременное и надлежащее рассмотрение всех заявлений о взаимодействии в связи с работой по ASN.1 и OID.

h) Создать дополнительные учебные курсы или веб-страницы, способные помочь пользователям ASN.1 и OID.

i) Получать согласие ОТК1/ПК6 и ИСО/МЭК и ИК17 на выделение любых дополнительных OID, которые будут сочтены необходимыми.

j) В рамках сферы ответственности руководителя проекта OID:

− предоставлять общие консультации пользователям OID;

− содействовать использованию ASN.1 и международных OID в других исследовательских комиссиях и внешних организациях по разработке стандартов (ОРС);

− помогать странам в создании и обеспечении работы национальных регистрационных органов для OID (включая международные OID).

## 3.3 Задачи, относящиеся к работе по поддержанию и ведению OSI

a) При необходимости подготовка исправлений или усовершенствований к Рекомендациям по OSI на основе полученных вкладов и исправление любых отмеченных недостатков;

b) Поддержание и ведение руководства для тех, кто занимается реализацией OSI.

## 3.4 Задачи, относящиеся к работе по поддержанию и ведению ODP

Подготовка исправлений к Рекомендациям по ODP или их доработка, по мере необходимости, на основе полученных вкладов и в целях исправления любых отмеченных недостатков.

# 4 Относящиеся к Вопросу

Рекомендации:

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

Вопросы:

• Все Вопросы МСЭ-Т, относящиеся к вышеупомянутым Рекомендациям

Исследовательские комиссии:

• ИК 2, 4, 11, 13, 16 и 20 МСЭ-Т и все исследовательские комиссии, которые используют ASN.1 или OID, либо у которых есть в них потребность

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, 204 ИСО; Организация по развитию стандартов структурированной информации (OASIS); Группа управления объектами (OMG); Консорциум World Wide Web (W3C)

Другие органы:

• Всемирный почтовый союз (ВПС)

ПРОЕКТ Вопроса L/17

Формальные языки для программного обеспечения
систем электросвязи и тестирования

(Продолжение Вопроса 12/17)

# 1 Обоснование

Настоящий Вопрос поддерживает непрерывную разработку различных формальных языков, широко используемых для проектирования и тестирования систем электросвязи.

Настоящий Вопрос охватывает определение и использование формальных языков проектирования систем МСЭ для определения требований, архитектуры и рабочих характеристик систем электросвязи: языков требований, описания данных, спецификации рабочих характеристик, тестирования и реализации. Формальные языки для этих областей разработки широко используются в отрасли и МСЭ-Т и поддерживаются коммерческими инструментами. Эти языки могут применяться, вместе или по отдельности, для спецификации стандартов и реализации продуктов. К языкам проектирования систем МСЭ относятся следующие языки.

• Нотация требований пользователя, которая применяется для анализа целей и определения сценариев использования, в особенности на начальных этапах проектирования.

• Абстрактная синтаксическая нотация №1 (ASN.1), оказавшаяся для большого числа групп по стандартизации предпочитаемой нотацией для спецификации информации, передаваемой между объектами, правила кодирования которой обеспечивают возможность однозначной, безопасной и эффективной передачи информации.

• Язык спецификации и описания, который позволяет определить воздействие на объекты и их реакцию и может сочетаться со спецификацией элементов данных в ASN.1.

• Профиль UML для языка спецификации и описания, который ограничивает модели UML четко определенным поведением, исключающим семантические вариации, присущие стандарту OMG, и отсутствует необходимость в частях UML, относящихся к поведению, которое охвачено языком спецификации и описания.

• Нотация диаграммы последовательности сообщений, обеспечивающая возможность описания последовательности сообщений, пересылаемых между объектами, которую можно также использовать для отслеживания поведения системы.

• Нотация тестирования и управления тестированием версии 3 (TTCN-3), которая дает 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.

• CHILL – язык программирования МСЭ-Т, который широко использовался в прошлом, но в последние годы применяются альтернативные методы, например генерация кода на основе языка спецификации и описания.

Все эти языки проектирования систем МСЭ определены в Рекомендациях в рамках настоящего Вопроса, за исключением ASN.1 (и ее соответствующих правил кодирования).

Наряду с определением языков документы в рамках настоящего Вопроса обеспечивают руководство по определению, использованию и применению языков (в том числе в некоторой степени ASN.1) для других исследовательских комиссий, внешних организаций по разработке стандартов и стран. В Рекомендациях МСЭ-т Z.110, Z.450, Z.500 и Z.Sup1 содержится руководство по использованию и применению языков. В Рекомендациях МСЭ-Т Z.111 и Z.119 содержатся руководящие принципы порядка составления любой новой Рекомендации по языку, и используются как включенные справочные документы в других Рекомендациях (в частности, в сериях Z.100 и Z.150).

В сферу охвата данного Вопроса по состоянию на 23 марта 2016 года входят следующие Рекомендации, Добавления и Руководства пользователя Рекомендации: X.292, 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.161, Z.161.1, Z.161.2, Z.161.3, Z.161.4, Z.161.5, Z.162, Z.163, Z.164, Z.165, Z.165.1, Z.166, Z.167, Z.168, Z.169, Z.170, Z.200, Z.450, Z.500, Z.Sup1 и Z.Imp100.

Разрабатываемые документы: не имеется.

# 2 Вопрос

Направления исследования, предназначенные для рассмотрения, включают, в том числе, следующие:

a) Какое необходимо сопровождение определений существующих языков проектирования систем (за исключением ASN.1), адаптированных к дополнительным современным требованиям пользователей и к появляющимся новым архитектурам и структурам?

b) Какие необходимы новые языки для дополнительных современных требований пользователей и появляющихся новых архитектур и структур (таких как интернет вещей), учитывая Рекомендацию МСЭ-Т Z.110?

# 3 Задачи

Задачи включают, в том числе, следующие:

i) осуществлять поддержание и ведение Рекомендаций, относящихся к сфере ответственности настоящего Вопроса;

ii) предоставлять общие консультации пользователям языка (языков), методики (методик), структуры (структур) для языка (языков), охватываемых исследуемым Вопросом;

iii) содействовать использованию методик, структур и языков, охватываемых исследуемым Вопросом, в других исследовательских комиссиях и внешних ОРС.

# 4 Относящиеся к Вопросу

Рекомендации:

• Серии X.680/X.690

Вопросы:

• K/17, все Вопросы МСЭ-Т, в которых используются языки проектирования систем

Исследовательские комиссии:

• ИК11, ведущая исследовательская комиссия по спецификациям тестирования и проверке на соответствие и функциональную совместимость, все исследовательские комиссии, использующие языки проектирования систем МСЭ (в частности, ИК 2, 11, 13, 16 и 20) или разрабатывающие спецификации тестов (в частности, ИК 2, 9, 11, 13, 15, 16 и 20), КГСЭ

Другие группы МСЭ-Т:

• JCA-CIT МСЭ-Т

Органы по стандартизации:

• Европейский институт стандартизации электросвязи (ЕТСИ) (ТК MTS); Целевая группа по инженерным проблемам интернета (IETF); ОТК1 ИСО/МЭК и все его подкомитеты, использующие языки проектирования систем МСЭ

Другие органы:

• Группа управления объектами (OMG); Сообщество форума SDL

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