|  |  |  |
| --- | --- | --- |
| **Всемирная ассамблея по стандартизации  электросвязи (ВАСЭ-20) Женева, 1−9 марта 2022 года** | |  |
|  | |  |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | Документ 10-R | | |
|  | Январь 2022 года | | |
|  | Оригинал: английский | | |
|  | | | |
| 11-я Исследовательская комиссия МСЭ-Т | | | |
| Требования к сигнализации, протоколы, спецификации тестирования И БОРЬБА С контрафактной продукцией | | | |
| ОТЧЕТ ИК11 МСЭ-Т ВСЕМИРНОЙ АССАМБЛЕЕ ПО СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ (васэ-20): ЧАСТЬ II – ВОПРОСЫ, ПРЕДЛАГАЕМЫЕ ДЛЯ ИССЛЕДОВАНИЯ В ходе СЛЕДУЮЩЕГО  ИССЛЕДОВАТЕЛЬСКОГО ПЕРИОДА (2022−2024 гг.) | | | |

|  |  |  |
| --- | --- | --- |
| **Резюме**: | В настоящем вкладе содержится текст Вопросов 11-й Исследовательской комиссии, предлагаемых для утверждения Ассамблеей на следующий исследовательский период. | |
| **Для контактов**: | г-н Андрей КУЧЕРЯВЫЙ Председатель ИК11 МСЭ-T Российская Федерация | Тел.: 79213140320 Эл. почта: [akouch@mail.ru](mailto:akouch@mail.ru) |

**Примечание БСЭ**:

Отчет 11-й Исследовательской комиссии для ВАСЭ-20 представлен в следующих документах:

Часть I: **Документ 9** – Общая информация

Часть II: **Документ 10** – Вопросы, предлагаемые для исследования в ходе исследовательского периода 2022−2024 годов

# 1 Список 14 Вопросов, предлагаемых 11-й Исследовательской комиссией

| Номер Вопроса | Название Вопроса | Статус |
| --- | --- | --- |
| A/11 | Сигнализация и архитектуры протоколов в сетях электросвязи и руководящие указания по реализации | Продолжение Вопроса 1/11 |
| B/11 | Требования к сигнализации и протоколы для управления услугами и приложениями в средах электросвязи | Продолжение Вопроса 2/11 |
| C/11 | Требования к сигнализации и протоколы для электросвязи в чрезвычайных ситуациях | Продолжение Вопроса 3/11 |
| D/11 | Протоколы для контроля сетевых ресурсов, управления ими и их оркестровки | Продолжение Вопросов 4/11 |
| E/11 | Требования к сигнализации и протоколы для шлюза пограничной сети в контексте виртуализации и интеллектуализации сети | Продолжение Вопроса 5/11 |
| F/11 | Протоколы, поддерживающие технологии контроля и управления для сетей IMT-2020 и дальнейших поколений | Продолжение Вопроса 6/11 |
| G/11 | Требования к сигнализации и протоколы подключения к сети и периферийных вычислений в будущих сетях и сетях IMT-2020 и дальнейших поколений | Продолжение Вопроса 7/11 |
| H/11 | Протоколы, поддерживающие организацию сетей распределенного контента и технологии информационно-ориентированной сети (ICN) для будущих сетей и сетей IMT-2020 и дальнейших поколений | Продолжение Вопроса 8/11 |
| I/11 | Тестирование интернета вещей, его приложений и систем идентификации | Продолжение Вопроса 12/11 |
| J/11 | Контроль параметров для протоколов, используемых в появляющихся сетях, включая облачные/периферийные вычисления и организацию сетей с программируемыми параметрами/виртуализацию сетевых функций (SDN/NFV) | Продолжение Вопроса 13/11 |
| K/11 | Тестирование облачных вычислений, SDN и NFV | Продолжение Вопроса 14/11 |
| L/11 | Борьба с использованием контрафактных и похищенных устройств электросвязи/ИКТ | Продолжение Вопроса 15/11 |
| M/11 | Спецификации тестирования протоколов, сетей и услуг для появляющихся технологий, включая оценочное тестирование | Продолжение Вопроса 16/11 |
| N/11 | Борьба с контрафактным и поддельным программным обеспечением электросвязи/ИКТ | Продолжение Вопроса 17/11 |

# 2 Формулировка Вопросов

В оставшейся части настоящего документа приводится предлагаемый текст Вопросов.

Вопрос А/11

Сигнализация и архитектуры протоколов в сетях электросвязи и руководящие указания по реализации

(Продолжение Вопроса 1/11)

### А.1 Обоснование

Желание поддержать услуги в рамках сетей и обеспечиваемых сетями привело к тому, что многочисленные органы и форумы по стандартизации приступили к разработке целого ряда архитектурных решений. Необходима стандартизированная архитектурная модель для управления сигнализацией в отношении передачи голоса и видеоизображений по сетям на базе LTE (VoLTE/ViLTE), виртуализации сети, облачных вычислений, МО/ИИ, технологии распределенного реестра, QKDN и связанных с ними технологий, а также других появляющихся технологий электросвязи/ИКТ, которые могут применяться в системах IMT-2020 и сетях IMT-2020 и дальнейших поколений.

Требуется стандартная эталонная модель для плоскости управления, чтобы определить набор интерфейсов, которые обеспечивают функциональную совместимость между сетями электросвязи, между оборудованием различных поставщиков, между сетями облачных вычислений, между виртуализированными и физическими сетями и между сетями, находящимися на разных этапах развития, такими как сети IMT-2020 и дальнейших поколений.

Поскольку МСЭ-Т занимается разработкой стандартов для существующих сетей связи общего пользования, включая услуги и протоколы управления, в рамках настоящего Вопроса планируется разработка сигнализации и архитектур протоколов для сетей электросвязи с применением появляющихся технологий, включая МО/ИИ, технологию распределенного реестра, QKDN и связанные с ними технологии и т. д. Кроме того, в рамках этого Вопроса будут изучаться усовершенствования в области сигнализации и архитектуры управления для поддержки системы сигнализации распределенного ENUM.

Требуется сотрудничество с исследовательскими комиссиями МСЭ-T и с другими организациями по разработке стандартов (ОРС) для сбора любой соответствующей информации от этих организаций и для того, чтобы играть важную роль в координации их деятельности для достижения глобальной функциональной совместимости.

Кроме того, проводимые исследования и результаты, достигнутые разными международными органами по стандартизации, привели к появлению различных решений, обеспечивающих конвергенцию и функциональную совместимость в результате изменения протоколов в сетях, основанных на коммутации пакетов. По этой причине Государства − Члены МСЭ, особенно развивающиеся страны, высказали необходимость содействия в понимании стратегий и сценариев развертывания сетей и услуг путем разработки руководящих указаний по внедрению протоколов сигнализации для сетей и услуг.

В рамках этого Вопроса будут вестись предыдущие Технические отчеты и Руководящие указания по внедрению сигнализации и протоколов, разработанные для оказания содействия развивающимся странам. Кроме того, в его рамках будут вестись действующие Рекомендации, за которые отвечает этот Вопрос, например Рекомендации МСЭ-Т Q.3030, Q.3040, Q.3050, Q. 3051 и Q.3052.

### А.2 Вопрос

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

– Какие усовершенствования сигнализации и архитектуры управления необходимы, для того чтобы моделировать плоскость управления сетей электросвязи с применением появляющихся технологий, таких как МО/ИИ, технология распределенного реестра, QKDN и связанные с ними технологии, а также технологии, применяемые в сетях IMT‑2020 и дальнейших поколений, с учетом новых услуг и новых приложений, а также всех видов проводных и беспроводных сетей доступа общего пользования, по которым могут предоставляться эти услуги?

– Какие усовершенствования сигнализации и архитектуры управления необходимы для поддержки системы сигнализации распределенного ENUM?

− Какие усовершенствования сигнализации и архитектуры управления необходимы для поддержки услуг VoLTE/ViLTE и IMT-2020, включая eMBB, mMTC и uRLLC, а также других новых дополнительных услуг?

– Какие усовершенствования сигнализации и архитектуры управления необходимы для обеспечения безопасности сигнализации и управления и для поддержки услуг и/или приложений, представляющих общественный интерес, таких как обработка экстренного вызова, переносимость номеров, конфиденциальность и т. д.?

– Какая требуется работа по подготовке Секторами МСЭ-T и МСЭ-D общих руководящих указаний, содержащих различные аспекты, которые относятся к стратегиям и сценариям развертывания сетей и услуг для поддержки внедрения протоколов сигнализации в сетях и услугах?

– Какие требуются механизмы координации в отношении сигнализации и разработки протоколов для появляющихся сетей электросвязи при сотрудничестве с исследовательскими комиссиями МСЭ-Т и другими организациями по разработке стандартов (ОРС)?

### А.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– определение требований, которые должны быть поддержаны общей архитектурой протоколов управления сигнализацией сетей электросвязи, независимой от технологий доступа. Ожидается, что эти требования необходимо будет периодически уточнять, для того чтобы отразить развитие технологий электросвязи и связи с использованием компьютеров с учетом архитектур протоколов управления сигнализацией, разработанных МСЭ-Т и другими ОРС;

– определение изменений и усовершенствований в архитектуре протоколов управления сигнализацией, которые позволят этой архитектуре удовлетворять требованиям архитектуры появляющихся сетей (включая системы IMT-2020, сети IMT-2020 и дальнейших поколений и т. д.);

− изучение архитектуры сигнализации и управления для моделирования плоскости управления сетей электросвязи с использованием появляющихся технологий, таких как МО/ИИ, технология распределенного реестра, QKDN и связанные с ними технологии, а также технологии, применяемые в сетях IMT-2020 и дальнейших поколений;

− поиск возможных усовершенствований архитектуры протоколов управления сигнализацией для поддержки системы сигнализации распределенного ENUM;

– определение усовершенствований в архитектуре протоколов управления сигнализацией в поддержку сетей электросвязи, развивающихся в направлении будущих сетей;

– определение набора интерфейсов, для которых желательно обеспечить функциональную совместимость и взаимодействие между различным сетевым оборудованием и для которых необходимо изучить подробные требования к сигнализации и разработать стандарты для протоколов управления;

– изучение и подготовка общих руководящих указаний, содержащих различные аспекты, которые относятся к стратегиям и сценариям развертывания сетей и услуг для поддержки внедрения протоколов сигнализации в сетях и услугах, особенно для содействия развивающимся странам;

– обеспечение связи и сотрудничества между исследовательскими комиссиями и форумами, относящимися к разработке сигнализации и протоколов для появляющихся сетей.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### А.4 Относящиеся к Вопросу

Рекомендации:

– Y.2012, Y.3015, Y.3510, Y.3104

Вопросы:

− Все Вопросы ИК11, особенно Вопросы, относящиеся к архитектурам и протоколам сигнализации

Исследовательские комиссии:

− ИК2, ответственная за различные аспекты ENUM

− ИК13, ответственная за архитектуру существующих и появляющихся сетей

− ИК15, ответственная за транспортировку

− ИК16, ответственная за мультимедийные услуги и кодирование

− ИК17, ответственная за структуру обеспечения безопасности

– ИК20, ответственная за IoT и его приложения

– ИК1 и ИК2 МСЭ-D

Другие органы:

– ATIS

– Форум по широкополосному доступу

– CCSA

– ЕТСИ

– IETF

– IEEE

– W3C

Направления деятельности ВВУИО:

– C2, C11

Цели в области устойчивого развития:

– 9

Вопрос B/11

Требования к сигнализации и протоколы для управления услугами и приложениями в средах электросвязи

(Продолжение Вопроса 2/11)

### В.1 Обоснование

По мере постоянного увеличения количества услуг и приложений непрерывно растет потребность в совершенствовании возможностей сетей электросвязи. Кроме того, такие технологии, как облачные вычисления, большие данные, DLT и машинное обучение/искусственный интеллект, QKDN и связанные с ними технологии, а также другие появляющиеся технологии электросвязи/ИКТ будут способствовать развитию новых протоколов сигнализации для обеспечения межсетевого взаимодействия и надлежащей связи в сетях IMT-2020 и дальнейших поколений. Эти появляющиеся технологии, а также дальнейшее развитие существующих технологий, безусловно, повлияют на стандартизацию сигнализации и протоколов.

Одна из целей развития сетей электросвязи состоит в том, чтобы надежным образом поддерживать широкий диапазон услуг: от услуг традиционной телефонии и интеллектуальных услуг до инновационных услуг, включающих услуги передачи звука, передачи данных, радиовещательной передачи изображений, а также диалоговые услуги, потоковые услуги, интерактивные игры, мобильные платежи/банковские услуги, приложения третьих сторон и т. д.

### В.2 Вопрос

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

– Какие протоколы сигнализации подходят для внедрения различных услуг и приложений в появляющейся среде электросвязи?

– Какие новые требования к сигнализации и протоколы необходимо разработать для поддержки услуг в сетях электросвязи, развивающихся в направлении сетей IMT-2020 и дальнейших поколений?

– Какие новые требования к сигнализации и протоколы необходимо разработать для поддержки услуг и приложений на основе появляющихся технологий электросвязи/ИКТ?

– Какие появляющиеся технологии, в том числе архитектуры и механизмы на основе QKDN и связанных с ними технологий, требуются для обеспечения безопасности сигнализации и управления, включая систему сигнализации № 7 (SS7) и появляющиеся системы сигнализации?

− Какие требования к сигнализации и протоколы необходимо разработать для поддержки услуг связи и обмена сообщениями в режиме реального времени?

− Какие новые требования к сигнализации и протоколы необходимо разработать для поддержки управления услугами электросвязи?

– Какие новые требования к сигнализации и протоколы требуются для поддержки услуг и/или приложений, представляющих общественный интерес, таких как мобильные платежи/банковские услуги, криптовалюта, мультимедийная связь в чрезвычайных ситуациях, конфиденциальность, переносимость номеров и т. д.?

### В.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– разработка требований к сигнализации и протоколов для внедрения различных услуг и приложений в среде электросвязи;

– разработка требований к сигнализации и протоколов для поддержки новых услуг в сетях электросвязи, развивающихся в направлении сетей IMT-2020 и дальнейших поколений;

– разработка требований к сигнализации и протоколов для поддержки услуг и приложений на основе появляющихся технологий;

– разработка требований к сигнализации и протоколов для поддержки услуг связи и обмена сообщениями в режиме реального времени;

– разработка систем безопасности сигнальной сети на основе появляющихся технологий, включая QKDN и связанные с ними технологии;

– разработка требований к сигнализации и протоколов для поддержки управления услугами электросвязи;

– разработка спецификаций для взаимодействия новых и существующих сигнализаций и протоколов;

– разработка требований к сигнализации и профилей протоколов, представляющих общественный интерес;

– совершенствование существующих протоколов сигнализации на основе установленных потребностей.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### В.4 Относящиеся к Вопросу

Рекомендации:

– Серия Q.600, серия Q.700, серия Q.900, серия Q.1900, серия Q.2700, серия Q.2900, серия Q.3400, серия Q.3500 и серия Q.3600

Вопросы:

− Все Вопросы ИК11

Исследовательские комиссии:

− ИК2, ответственная за аспекты управления сетями и связь в чрезвычайных ситуациях

− ИК13, ответственная за требования к услугам, аспекты архитектуры, облачные вычисления и мобильность

− ИК15, ответственная за "умные" электросети

− ИК16, ответственная за мультимедийные услуги и приложения

− ИК17, ответственная за аспекты безопасности

– ИК20, ответственная за IoT и его приложения

Другие органы:

– ARIB

– ATIS

– Форум по широкополосному доступу

– CCSA

– ЕТСИ

– IETF

– IEEE

– TIA

– TTA

– TTC

Направления деятельности ВВУИО:

– C2, C5, C11

Цели в области устойчивого развития:

– 9

Вопрос C/11

Требования к сигнализации и протоколы для электросвязи   
в чрезвычайных ситуациях

(Продолжение Вопроса 3/11)

### С.1 Обоснование

В появляющейся сетевой среде потребуется изучить воздействие вновь появляющихся технологий, возможностей и прикладных услуг (например, сетей IMT-2020 и дальнейших поколений, конвергенции наземных и спутниковых сетей, передачи видеоизображения и голоса по сети LTE (VoLTE/ViLTE), межмашинной связи (M2M), интернета вещей (IoT), технологии распределенного реестра, машинного обучения/искусственного интеллекта, QKDN и связанных с ними технологий) на электросвязь в чрезвычайных ситуациях, в том числе на службу электросвязи в чрезвычайных ситуациях (ETS). Кроме того, необходимо исследовать, как можно воспользоваться некоторыми появляющимися технологиями и прикладными услугами в интересах электросвязи в чрезвычайных ситуациях.

Необходимо также продолжать разработку приложений для электросвязи в чрезвычайных ситуациях, например требований к передаче голоса, изображений и сигнализации данных и усовершенствований протоколов.

Этот Вопрос отвечает за обеспечение поддержания существующих возможностей ETS в Добавлениях и Рекомендациях ИК11, например Q.931, Q.761, Q.762, Q.763, Q.764, Q.1902.1, Q.1902.3, Q.1902.4, Q.1950, Q.2630.3, Q.2931, Добавлении 47 серии Q, Добавлении 49 серии Q для конкретной информации о ETS, Добавлении 53 серии Q, Добавлении 57 серии Q, Добавлении 61 серии Q, Добавлении 62 серии Q, Добавлении 63 серии Q, Добавлении 68 серии Q, Добавлении 69 серии Q и Добавлении 70 серии Q.

В рамках этого Вопроса будет осуществляться взаимодействие с региональными ОРС, занимающимися электросвязью в чрезвычайных ситуациях или возможностями, требующимися для ее реализации. Например, усовершенствования 3GPP в отношении приоритетных сообщений; разработка технических решений IETF для методов управления перегрузками, все из которых будут содействовать внедрению приоритетных сообщений для пользователей электросвязи в чрезвычайных ситуациях; усовершенствования IEEE в отношении серии стандартов IEEE 802.11, которые применяются к пользователям электросвязи в чрезвычайных ситуациях.

### С.2 Вопрос

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

− Какие требования к сигнализации и усовершенствования протоколов необходимо определить в поддержку электросвязи в чрезвычайных ситуациях и оказания помощи при бедствиях в сетях IMT-2020 и дальнейших поколений?

− Какие требования к сигнализации и протокол необходимо определить для поддержки электросвязи в чрезвычайных ситуациях и оказания помощи при бедствиях для конвергенции наземных и спутниковых сетей?

− Какие Рекомендации должны быть разработаны в ответ на эти требования, поскольку данная работа не охвачена другими Вопросами в настоящей ИК?

− Какие изменения следует предложить к общим планам, поддерживаемым соответствующими ведущими исследовательскими комиссиями, для того чтобы создать новые возможности, обеспечить более эффективную реализацию возможностей, которые уже находятся в процессе стандартизации, или устранить устаревшее содержание?

### С.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

− анализ возможностей электросвязи в чрезвычайных ситуациях, которым соответствующие ведущие исследовательские комиссии уделяют первоочередное внимание для того, чтобы определить конкретные задачи для исследования, которые должны быть добавлены в планы работы отдельных Вопросов ИК;

− создание условий для того, чтобы между Вопросами Исследовательской комиссии на техническом уровне была налажена необходимая связь, обеспечивающая эффективность, согласованность и полноту работы по реализации возможностей электросвязи в чрезвычайных ситуациях;

− создание условий для того, чтобы на техническом уровне была налажена необходимая связь между Вопросами Исследовательской комиссии, Вопросами других исследовательских комиссий и другими группами, разрабатывающими стандарты, касающиеся электросвязи в чрезвычайных ситуациях, как это определено в планах, принятых соответствующими ведущими исследовательскими комиссиями;

− анализ возможностей, связанных с ETS и оказанием помощи при бедствиях, уже отраженных в Рекомендациях в пределах сферы ответственности Исследовательской комиссии, для обеспечения того, чтобы они оставались актуальными и эффективными;

− содействие разработке и ведению планов, относящихся к сфере ответственности соответствующих ведущих исследовательских комиссий по электросвязи в чрезвычайных ситуациях, включая предложение нового содержания, когда это представляется целесообразным;

− разработка Добавлений и Рекомендаций, определяющих требования к сигнализации и протоколы в поддержку электросвязи в чрезвычайных ситуациях и оказания помощи при бедствиях в сетях IMT-2020 и дальнейших поколений;

− разработка Добавлений и Рекомендаций, определяющих требования к сигнализации и протоколы в поддержку электросвязи в чрезвычайных ситуациях и оказания помощи при бедствиях при конвергенции наземных и спутниковых сетей.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### С.4 Относящиеся к Вопросу

Рекомендации:

– Работа, за которой осуществляется надзор по линии данного Вопроса, ведется в рамках, определенных Рекомендацией МСЭ-T Y.1271 и Рекомендацией МСЭ-T Y.2205

Вопросы:

− Все Вопросы ИК11

Исследовательские комиссии:

Вопросы будут относиться к следующим исследовательским комиссиям, особенно в том что касается Вопросов, конкретно касающихся электросвязи в чрезвычайных ситуациях:

– ИК2 МСЭ-T

– ИК9 МСЭ-T

– ИК13 МСЭ-T

– ИК16 МСЭ-T

– ИК17 МСЭ-T

– ИК20 МСЭ-T

Другие органы:

– ARIB

– ATIS

– IETF

– IEEE

− ЕТСИ

– TIA

– TTA

– TTC

Направления деятельности ВВУИО:

– C2, C5

Цели в области устойчивого развития:

– 9, 11, 13, 16

Вопрос D/11

Протоколы для контроля сетевых ресурсов, управления ими и их оркестровки

(Продолжение Вопроса 4/11)

### D.1 Обоснование

В рамках деятельности по данному Вопросу была разработана серия Рекомендаций по контролю, администрированию и оркестровке ресурсов несущей сети, относящихся к моделям данных, требованиям к сигнализации и протоколам. Ожидается, что стандартизация вышеупомянутого аспекта, включая, помимо прочего, сети с программируемыми параметрами (SDN), виртуализацию сетевых функций (NFV), сети облачных вычислений, "нарезку" сети, сети IMT-2020 и дальнейших поколений, виртуализацию сетей, переход к IPv6, будущие сети (FN), продолжится и распространится на новые области исследований МСЭ-T, такие как искусственный интеллект/машинное обучение (ИИ/МО) и сети, управляемые большими данными, технология распределенного реестра, распределенные облачные вычисления, периферийные вычисления с множественным доступом (MEC), сети вычислительных мощностей и другие появляющиеся ИТ с поддержкой технологий несущей сети.

Поведение трафика, создаваемого все новыми и новыми услугами, такими как услуги, предоставляемые SDN, NFV, сети облачных вычислений и другие появляющиеся ИТ с поддержкой технологий несущей сети, весьма отличается от поведения трафика, создаваемого традиционными услугами СПП. Соответственно, архитектура для управления таким новым трафиком может стать более сложной. Требования к сигнализации в несущих сетях тесно связаны с механизмами и протоколами управления сетевыми ресурсами.

Действующие Рекомендации, за которые отвечает данный Вопрос: Q.1970, Q.1990, Q.2630, Q.2761−2764, Q.2920, Q.2931 и Q.2932.1, Q.3150/Y.1416, Q.3151/Y.1417, Q.3300, Q.3301.1, Q.3302.1, Q.3303.0, Q.3303.1, Q.3303.2, Q.3303.3, Q.3304.1, Q.3304.2, Q.Доб.51, Q.Доб.67, Q.3316, Q3405, Q.3716, Q.3718, Q.3740, Q.3741.

### D.2 Вопрос

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

– Какие модели данных, требования к сигнализации и протоколы необходимы для контроля, администрирования и оркестровки сетевых ресурсов, включая новые типы транспортных протоколов и транспортных сетей (такие, как сети облачных вычислений, интеллектуальные сети, FN, SDN, NFV, виртуализация сетей, "нарезка" сетей, MEC и сети IMT-2020 и дальнейших поколений)?

− Какие модели данных, требования к сигнализации и протоколы необходимы для сетей на основе больших данных и ИИ/МО?

– Какие модели данных, требования к сигнализации и протоколы необходимы для сетевой телеметрии?

– Какие модели данных, требования к сигнализации и протоколы необходимы для сетей с поддержкой технологии распределенного реестра?

– Какие модели данных, требования к сигнализации и протоколы необходимы для сетей на основе облачных вычислений и распределенных облачных вычислений?

– Какие модели данных, требования к сигнализации и протоколы необходимы для сетей вычислительных мощностей?

− Какие новые Рекомендации требуются для поддержки управления каналом-носителем и ресурсами для новых областей применения, таких как одноадресные/многоадресные потоки для услуги IPTV, организация домашних сетей и мобильность?

− Какие новые Рекомендации требуются для поддержки управления передачей обслуживания для мобильности?

− Какие новые Рекомендации требуются для обеспечения безопасности сигнализации по каналу-носителю и ресурсов управления им?

− Какие новые усовершенствования функциональной архитектуры и протоколов необходимы для поддержки управления каналом-носителем и ресурсами для услуг и приложений, представляющих общественный интерес, таких как обработка экстренного вызова и оказание помощи при бедствиях?

− Какие новые Рекомендации требуются для поддержки сигнализации информации о качестве обслуживания (QoS), управления трафиком?

– Какие усовершенствования существующих Рекомендаций требуются для прямого или косвенного обеспечения экономии энергии и эффективного использования ресурсов в отрасли информационно-коммуникационных технологий или других отраслях?

– Какие усовершенствования новых Рекомендаций требуются для обеспечения такой экономии энергии и эффективного использования ресурсов?

– Какие можно определить новые услуги, для которых необходимым условием является внедрение IPv6?

– Какие новые процедуры протокола необходимо разработать для внедрения указанных выше услуг?

– Какие требуются новые Рекомендации по информационной модели и модели данных для сотрудничества с появляющимися сообществами разработчиков программного обеспечения с открытым исходным кодом?

### D.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

− разработка моделей данных, требований к сигнализации и протоколов для новых услуг по каналу-носителю для поддержки трафика новых приложений на основе архитектур будущих сетей, включая SDN, NFV, виртуализацию сетей, MEC, "нарезку" сетей, сети на основе облачных вычислений и распределенных облачных вычислений, сети IMT-2020 и дальнейших поколений и т. д.;

− разработка моделей данных, требований к сигнализации и протоколов для сетей на основе больших данных и ИИ/МО;

– разработка моделей данных, требований к сигнализации и протоколов для сетевой телеметрии;

– разработка моделей данных, требований к сигнализации и протоколов для сетей на основе облачных вычислений и распределенных облачных вычислений;

– разработка моделей данных, требований к сигнализации и протоколов для сетей, поддерживающих технологию распределенного реестра, включая децентрализованную надежную сетевую инфраструктуру (DNI);

– разработка моделей данных, требований к сигнализации и протоколов для сетей вычислительных мощностей;

− разработка требований к сигнализации и протоколов для координации управления доступом;

− разработка требований к сигнализации и протоколов для контроля за каналом-носителем и ресурсами и управления трафиком в поддержку одноадресных/многоадресных потоков для услуги IPTV;

− разработка требований к сигнализации и протоколов для управления сигнализацией QoS и трафиком;

− разработка требований к сигнализации и протоколов для управления каналом-носителем и ресурсами в поддержку организации домашней сети;

− разработка требований к сигнализации и протоколов в поддержку передачи обслуживания для плавной мобильности сеанса;

− разработка требований к сигнализации и протоколов для взаимодействия между доменами управления каналом-носителем и ресурсами;

− разработка спецификаций интерфейсов со смежными уровнями совместно с соответствующими Вопросами/группами ИК МСЭ-T;

− совершенствование существующих Рекомендаций, касающихся управления каналом-носителем и ресурсами и сигнализации;

− проведение исследований и разработка Рекомендаций в целях определения требований к механизмам управления каналом-носителем и сигнализации в зависимости от услуг;

− определение услуг, для которых необходимы новые процедуры протокола для перехода к IPv6;

− разработка новых процедур протокола для указанных выше услуг;

− разработка информационной модели и модели данных на основе требований к сигнализации и протоколов для их внедрения в будущем с использованием программного обеспечения с открытым исходным кодом.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### D.4 Относящиеся к Вопросу

Рекомендации:

− H.248, Q.1950, Y.1541, Y.1221, Y.2111, I.555, Q.1970, Q.1990, серия Q.263x, серия Q.29xx, Y.2121, Y.3300, серия Y.35xx, серия Q.37xx, серия Q.33xx, серия Q.34xx.

Вопросы:

– Все Вопросы ИК11

Исследовательские комиссии:

− ИК15, ответственная за технологии транспорта и АКТС, прежде всего за архитектуры транспортных сетей и управление и контроль транспортных систем и оборудования

− ИК16, ответственная за аспекты мультимедиа и ИИ

− ИК17, ответственная за аспекты безопасности

− ИК13, ответственная за SDN, NFV, организацию сетей облачных вычислений и распределенных облачных вычислений, виртуализацию сетей, "нарезку" сетей, MEC, сети, управляемые большими данными, сети на основе ИИ/МО и сети IMT-2020 и дальнейших поколений

Другие органы:

− 3GPP

– ЕТСИ

– IEEE

– IETF

– TIA

− Linux Foundation Edge

– Linux Foundation Networking (LFN)

– Linux Foundation Hyperledger

– OpenStack

– Open Network Operating System

Направления деятельности ВВУИО:

– C2, C11

Цели в области устойчивого развития:

– 9

Вопрос E/11

Требования к сигнализации и протоколы для шлюза пограничной сети в контексте виртуализации и интеллектуализации сети

(Продолжение Вопроса 5/11)

### Е.1 Обоснование

С появлением новых технологий, таких как SDN, NFV, облачные вычисления, интернет вещей и искусственный интеллект, особенно с развитием сетевой архитектуры в направлении виртуализации, открытости и интеллектуализации, происходит постоянное совершенствование формы устройств и развертывание сервисных функций шлюза пограничной сети (BNG), в свою очередь инициирующие развитие сети доступа пользователей и предоставления услуг. Следовательно, чтобы адаптироваться к эволюции сетевой архитектуры, необходимо определить новые требования к услугам, интерфейсы и протоколы сигнализации для шлюза пограничной сети в целях поддержки многих услуг, а также расширить возможности BNG в целях обеспечения лучшего качества обслуживания и повышения надежности и безопасности для доставки многих услуг.

При внедрении в сеть доступа технологии организации сетей с программируемыми параметрами (SDN), виртуализации сетевых функций (NFV) и технологии интеллектуальных сетей требуется определить новые интерфейсы, чтобы открыть возможности сети, определить новый протокол для управления лежащими в основе устройствами физической передачи, определить новый интерактивный процесс для протоколов в целях обеспечения связи между контроллером и устройствами передачи, определить новые протоколы и процедуры для повышения надежности, лучшего использования ресурсов и гибкого распространения политики пользователей между многочисленными BNG. Также новые процедуры протокола требуются для обеспечения оперативного предоставления услуг по клиентским IP-сетям, услуг клиенту через многочисленные шлюзы пограничной сети и дополнительных услуг (VAS) по организации открытых сетей.

С появлением новых технологий также постепенно развивается сетевая архитектура операторов. Требуется, чтобы шлюз пограничной сети обладал возможностями по доставке многих услуг и реализовывал такие функции, как сеть фиксированной связи (например, BRAS), сеть подвижной связи (например, шлюз PDN), шлюз услуг IoT, шлюз сети связи космос-земля и т. д. Функции BNG могут быть реализованы путем загрузки функций виртуальной сети (VNF) в виртуализированную облачную инфраструктуру электросвязи. Необходимо изучить функциональные требования к шлюзу пограничной сети в соответствии с различными сценариями, процессы контроля доступа пользователей, распределения и предоставления услуг, протокол сигнализации и механизм обеспечения QoS для гибкого планирования ресурсов при различных требованиях к скорости передачи и функциям безопасности.

Кроме того, для реализации операций автоматизации сети и эффективного и гибкого планирования сетевых ресурсов в сеть внедряются технологии искусственного интеллекта. Для принятия решений по интеллектуальному управлению, чтобы предоставить пользователям гарантию повышенного QoS, необходимо собирать данные о состоянии сети от ключевых элементов сети (например, BNG) по всей сети в режиме реального времени. Необходимо определить модель данных, процесс взаимодействия данных и протокол сигнализации, чтобы центр принятия решений ИИ получал данные о состоянии сети в режиме реального времени и передавал в элементы сети (например, BNG) оптимизированную политику для реализации эффективной доставки услуг пользователям.

### Е.2 Вопрос

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

– Какие новые протоколы и процедуры необходимо определить, чтобы обеспечить оперативное предоставление услуг в клиентских IP-сетях с использованием появляющихся технологий (например, SDN/NFV, облачных вычислений, IoT, ИИ, MEC и т. д.)?

– Какие новые протоколы и процедуры необходимо определить, чтобы доставлять клиентам услуги и политику через шлюзы широкополосной сети с использованием появляющихся технологий?

– Какие новые протоколы и процедуры необходимо определить для реализации сети вычислительных мощностей между многими шлюзами пограничной сети?

– Какие новые интерфейсы, протоколы и функции шлюза пограничной сети необходимо реализовать для поддержки появляющихся технологий?

– Какие новые интерфейсы, протоколы и функции шлюза пограничной сети необходимо реализовать для поддержки конвергенции нескольких технологий доступа к сети (включая фиксированный доступ, подвижный доступ, IoT-доступ, доступ через спутниковую сеть и т. д.)?

– Какие новые механизмы, протоколы и процедуры необходимо определить для распространения политики пользователей по контролю за доступом пользователей и обеспечению QoS пользователей?

– Какие новые протоколы и процедуры необходимо определить для обеспечения дополнительных услуг (VAS) по организации открытой сети?

– Какие новые протоколы и процедуры необходимо определить в шлюзе пограничной сети для доставки многих услуг?

− Какие новые протоколы и процедуры необходимо определить, чтобы обеспечить управление сетью и оркестровку ресурсов между несколькими шлюзами пограничной сети с помощью ИИ?

– Какие новые модель данных, протокол и процесс взаимодействия следует определить, чтобы позволить центрам принятия решений на основе ИИ получать от шлюзов пограничной сети данные о состоянии в режиме реального времени?

### Е.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– разработка описаний услуг для услуг, не описанных другими ОРС, и при необходимости определение терминов;

– разработка новых протоколов и процедур для обеспечения оперативного предоставления услуг по клиентским IP-сетям;

– разработка новых протоколов и процедур для обеспечения обслуживания клиента через шлюзы пограничной сети с применением появляющихся технологий;

– разработка новых протоколов и процедур для реализации сети вычислительных мощностей между многими шлюзами пограничной сети;

− разработка новых требований, протоколов и функций для шлюза пограничной сети в целях поддержки появляющихся технологий (таких, как SDN/NFV, облачные вычисления, IoT, ИИ, MEC и т. д.);

– разработка новых требований, протоколов и функций для шлюза пограничной сети в целях поддержки конвергенции сетевых технологий множественного доступа (включая фиксированный доступ, подвижный доступ, IoT-доступ, доступ через спутниковые сети и т. д.);

– разработка новых протоколов и процедур для шлюза пограничной сети в целях повышения эффективности использования сетевых ресурсов с помощью интеллектуального управления сетью;

– разработка новых протоколов и процедур для обеспечения управления и распространения политики пользователей с помощью технологий SDN;

– разработка новых протоколов и процедур для обеспечения дополнительных услуг (VAS) по организации открытой сети;

– разработка новых протоколов и процедур для доставки многих услуг по BNG;

– разработка методики тестирования безопасности и спецификации тестов для тестирования безопасности процедур протокола, относящихся к услугам, предоставляемым шлюзами широкополосной сети;

− разработка нового протокола и процедур, позволяющих реализовать управление сетью и оркестровку ресурсов между несколькими шлюзами пограничной сети с помощью ИИ.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### Е.4 Относящиеся к Вопросу

Рекомендации:

− Серии Q, Y и H

Вопросы:

− Вопрос А/11, Вопрос В/11 и Вопрос D/11 по управлению политикой

− Вопрос C/11, Вопрос G/11 и Вопрос M/11

Исследовательские комиссии:

− ИК13 МСЭ-T и другие ИК, работающие над СПП, будущими сетями, сетями IMT-2020 и шлюзами широкополосной сети

− ИК20 МСЭ-T

Другие органы:

– Форум по широкополосному доступу

– IETF

− ЕТСИ

Программное обеспечение с открытым исходным кодом:

– ONAP

Направления деятельности ВВУИО:

– C2

Цели в области устойчивого развития:

– 9

Вопрос F/11

Протоколы, поддерживающие технологии контроля и управления для сетей IMT-2020 и дальнейших поколений

(Продолжение Вопроса 6/11)

### F.1 Обоснование

В рамках деятельности по данному Вопросу был разработан ряд протоколов для технологий контроля и управления, таких как оркестровка, "нарезка" сети, представление возможностей сети, идентификация и управление сетью в разнородных сетевых средах, в целях реализации сети IMT‑2020.

Применение искусственного интеллекта (ИИ) для обеспечения автоматизации и интеллектуального управления сетью – важная тема в наши дни. Для удовлетворения требований рынка следует срочно определить и описать, каким образом следует применять технологии ИИ и больших данных для поддержки интеллектуального контроля и управления в сетях IMT-2020 и дальнейших поколений. В частности, следует разработать протоколы для поддержки интеллектуального управления в сетях IMT-2020 и дальнейших поколений, усовершенствованные механизмы, обеспечивающие короткую задержку, низкий уровень дрожания и потери пакетов, гарантированную полосу пропускания, сверхбольшую сеть, гибкое установление соединения и гибкую топологию, выделение и распределение ресурсов, а также "нарезку" сети, присвоив этим разработкам высокий приоритет. В связи с особыми требованиями вертикальных отраслей следует усовершенствовать управление плоскостью пользователя в целях оптимизации пользовательского тракта и выполнения отраслевых требований.

Другие важные проблемы, которые необходимо решить в будущем, – создание протоколов единой системы управления для работы с сетями как фиксированной, так и подвижной связи.

### F.2 Вопрос

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

– Какие протоколы и механизмы необходимо определить в ответ на анализ пробелов, который проводили соответствующие ОРС?

– Какие протоколы и механизмы необходимо определить в поддержку сценариев услуг, требований, функциональных возможностей и архитектуры для сетей IMT-2020 и дальнейших поколений, разработанных соответствующими ИК МСЭ-T и другими ОРС?

– Какие протоколы и механизмы необходимо определить для ключевых технологий, применяемых при реализации сетей IMT-2020 и дальнейших поколений, включая интеллектуальное управление транспортной сетью, оркестровку, "нарезку" сети, оптимизацию плоскости пользователей, представление возможностей сети, идентификацию, аутентификацию устройств, конвергенцию фиксированной и подвижной связи, сетевое управление разнородными сетевыми средами и т. д.?

– Как появляющиеся технологии, включая искусственный интеллект, большие данные, а также QKDN и связанные с ними технологии, используются в протоколах контроля и управления для сетей IMT-2020 и дальнейших поколений?

– Какие протоколы и механизмы следует определить для реализации высоких показателей работы сетей IMT-2020 и дальнейших поколений с такими характеристиками, как сверхкороткая задержка и высокая надежность?

– Какие протоколы и механизмы следует определить для реализации улучшений и усовершенствований интерфейса на основе услуг для сети IMT-2020 в целях повышения ее эффективности, гибкости и интеллекта?

– Как использовать программное обеспечение с открытым исходным кодом и направлять его разработку в сотрудничестве с соответствующими организациями, имеющими отношение к созданию ключевых технологий сетей IMT-2020 и дальнейших поколений, в целях реализации разработанных Рекомендаций?

### F.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

− разработка Рекомендаций по протоколам, включая механизмы, для контроля сетей IMT‑2020 и дальнейших поколений с расширенными функциями, поддерживающими сверхбольшую сеть, гибкое установление соединений и гибкую топологию, конвергенцию фиксированной и подвижной связи, оптимизацию плоскости пользователя и т. д.;

– разработка Рекомендаций по протоколам, включая механизмы, для поддержки сети IMT‑2020 и дальнейших поколений с использованием таких технологий, как "нарезка" сети, виртуализация ресурсов, оркестровка, искусственный интеллект и большие данные, QKDN и связанные с ними технологии и т. д.;

– разработка Рекомендаций по протоколам, включая механизмы, для других ключевых технологий IMT-2020 и дальнейших поколений, включая идентификацию, аутентификацию устройств, представление возможностей сети и др.;

– разработка Рекомендаций по протоколам, включая механизмы, для общей системы управления сетями IMT-2020 и дальнейших поколений;

– разработка Рекомендаций по протоколам, включая механизмы, для сети IMT-2020 в целях достижения высоких показателей работы с такими характеристиками, как сверхкороткая задержка и высокая надежность;

– разработка Рекомендаций по протоколам для сетей IMT-2020 и дальнейших поколений в целях реализации улучшений и усовершенствований интерфейса на основе услуг для повышения эффективности, гибкости и интеллекта;

– разработка, в сотрудничестве с соответствующими органами, Добавления, Технического отчета, Руководящих указаний по передовому опыту и реализации протоколов и механизмов для сетей IMT-2020 и дальнейших поколений, в том числе программного обеспечения с открытым исходным кодом.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### F.4 Относящиеся к Вопросу

Рекомендации:

– Серия Y и серия Q

Вопросы:

– Вопросы D/11, G/11, H/11, K/11

Исследовательские комиссии:

– 2-я Исследовательская комиссия МСЭ-Т

– 13-я Исследовательская комиссия МСЭ-Т

– 15-я Исследовательская комиссия МСЭ-Т

– Другие ИК, участвующие в исследованиях IMT-2020

Другие органы:

– МСЭ-R

– ЕТСИ

– IETF

– IEEE

– 3GPP

Направления деятельности ВВУИО:

– C2, C5

Цели в области устойчивого развития:

– 9, 17

Вопрос G/11

Требования к сигнализации и протоколы подключения к сети и периферийных вычислений в будущих сетях и сетях IMT-2020 и дальнейших поколений

(Продолжение Вопроса 7/11)

### G.1 Обоснование

МСЭ-T провел исследование требований к сигнализации и протоколов для будущих сетей. Актуальными темами были периферийные вычисления, необходимые для искусственного интеллекта, больших данных, автономных транспортных средств и роботов, поскольку в этот период началась коммерческая эксплуатация сетей IMT-2020.

Будущие сети и сети IMT-2020 охватят широкий спектр услуг (мультимедиа, зондирование, искусственный интеллект, большие данные, мобильность, роботы и т. д.), включая аспекты конвергенции, основанные на их высокой вычислительной мощности и способности периферийных сетей обслуживать разнородные сети (IMT-2020, LTE, 3G, WLAN, BLE, LPWA и т. д.), множество устройств (смартфоны, планшеты, ноутбуки, датчики, CCTV и т.д.) и среду облачных вычислений (периферийные облачные вычисления, общедоступные облачные вычисления и т. д.) в динамическом сочетании разнообразных возможностей для совместной работы. Речь идет о так называемых периферийных вычислениях, и, как ожидается, протоколы сигнализации соединят источник и устройство для их реализации. Они будут включать федеративную аутентификацию и конфигурацию для динамической передачи мультимедийных данных, посеансовое распределение IP-адресов и конфигурацию терминала, проверку авторизации доступа к сети, внутрисеансовое изменение возможности установления соединений, управление подсоединением и распределение ресурсов для периферийных вычислений.

Кроме того, IMT-2020 может повысить скорость трафика пакетов данных в десять раз по сравнению с сетями 4G, тогда как периферийные вычисления сокращают задержку транзакций благодаря размещению вычислительных мощностей в сети IMT-2020 ближе к конечным пользователям подвижной связи. В этой связи возможности облачных вычислений также важны для обеспечения транзакций данных со сверхкороткой задержкой для услуг, требующих короткой задержки и высокой пропускной способности (дополненная/виртуальная реальность (AR/VR), потоковое мультимедиа, "Индустрия 4.0", роботы, IoT и т. д.). Эти процедуры следует разрабатывать с учетом различных появляющихся услуг, таких как AR/VR, потоковые игры, ИИ, большие данные, автономные транспортные средства, роботы и т. д.

Для повышения разнообразия услуг и способностей устройств также необходимо максимальное использование ресурсов и управление на основе информированности. Соответственно, необходимо учитывать основные аспекты будущих сетей, такие как виртуализация и сети с программируемыми параметрами (SDN), интеллектуальные периферийные вычисления (IEC), периферийные вычисления с множественным доступом (MEC) и облачные услуги для сети доступа.

### G.2 Вопрос

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

– Какие новые и пересмотренные Рекомендации требуются для работы над пересмотрами требований к протоколам сигнализации NACF?

– Какие новые Рекомендации необходимы для определения требований к сигнализации и протоколов в поддержку услуг присоединения и периферийных вычислений (ИИ, большие данные, мобильность, периферийные облачные вычисления и т. д.) для услуг с использованием нескольких устройств/интерфейсов/соединений?

– Какие соответствующие механизмы требуются при сигнализации присоединения и периферийных вычислений для обеспечения безопасности для услуг с использованием нескольких устройств/интерфейсов/соединений?

– Какие механизмы контроля требуются при сигнализации присоединения и периферийных вычислений для поддержки управления мобильностью и управления виртуальными ресурсами?

− Какая функциональная архитектура и какие объекты требуются для присоединения к сетям и периферийных вычислений для поддержки будущих сетей и сети IMT-2020, включая SDN, NFV, IEC и MEC в сети доступа?

− Какая функциональная архитектура и какие объекты требуются для поддержки услуг потоковой передачи с использованием нескольких интерфейсов, специализирующихся на сигнализации присоединения доступа и протоколах?

### G.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– ведение существующих Рекомендаций, изучаемых в рамках данного Вопроса;

– разработка требований к сигнализации и протоколов для поддержки пересмотра требований к протоколу присоединения к сетям и периферийных вычислений;

− разработка требований к сигнализации и протоколов для поддержки процедур присоединения к сетям и периферийных вычислений с использованием нескольких устройств, нескольких соединений и нескольких интерфейсов для будущих сетей (например, SDN, NFV) и сетей IMT-2020 и дальнейших поколений;

– разработка требований к сигнализации и протоколов для поддержки функций управления мобильностью и управления ресурсами как в сетях доступа, так и в базовых сетях;

– разработка требований к сигнализации и протоколов для поддержки разнообразных и эффективных схем классификации трафика и управления трафиком на основе устройств с поддержкой MEC (уровень с поддержкой MEC, IEC, SDK и т. д.), базовой сети ("нарезка" сети, APN и т. д.) и управления периферийным оборудованием (периферийные облачные вычисления и т. д.) для сетей с гарантированной короткой задержкой IMT-2020 и дальнейших поколений;

– разработка требований к сигнализации и протоколов для поддержки управления мобильностью и переноса услуг/приложений в среду с поддержкой периферийных вычислений и облачных периферийных вычислений, включая поддержку распределения вычислительных ресурсов, распределения ресурсов с учетом мобильности и отказоустойчивости для маршрутизации трафика ближайшей периферии в будущих сетях и сетях IMT-2020 и дальнейших поколений.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### G.4 Относящиеся к Вопросу

Рекомендации:

– Рекомендации серии Y по требованиям и архитектурам будущих сетей и сетей IMT‑2020 и дальнейших поколений

– Рекомендации серии Q по требованиям, протоколам, измерениям и тестированию, относящимся к сигнализации

Вопросы:

– Вопросы A/11, B/11, D/11, M/11, F/11

Исследовательские комиссии:

− ИК13, ответственная за требования к будущим сетям и сетям IMT-2020 и дальнейших поколений, их архитектуру, управление мобильностью и виртуализацию ресурсов

– ИК16, ответственная за мультимедийные услуги в среде с несколькими устройствами/интерфейсами/соединениями

– ИК20, ответственная за услуги и протоколы M2M и IoT

– ИК17, ответственная за аспекты безопасности и управление определением идентичности

Другие органы:

– РГ7 ОТК1 ИСО/МЭК

– IETF

– OMA

− ЕТСИ

Направления деятельности ВВУИО:

– C2

Цели в области устойчивого развития:

– 9

Вопрос Н/11

Протоколы, поддерживающие организацию сетей распределенного контента и технологии информационно-ориентированной сети (ICN) для будущих сетей и сетей IMT-2020 и дальнейших поколений

(Продолжение Вопроса 8/11)

### Н.1 Обоснование

Для появляющихся мультимедийных услуг и приложений требуются различные функции и возможности. Функции сквозной многоадресной передачи являются одной из основных характеристик мультимедийных приложений с возможностью осуществлять связь со многими сторонами. Исходя из данного обоснования был разработан набор Рекомендаций МСЭ-Т по структуре и протоколам управления группой и сквозной многоадресной связи в сетевой среде многоадресной передачи на базе IP и без поддержки IP. В результате сотрудничества с ПК6 ОТК1 ИСО/МЭК были разработаны многие общие тексты стандартов для многосторонней связи, и они включают серию X.606 МСЭ-Т | серию 14476 ИСО/МЭК, серию X.607 МСЭ-Т | серию 14476 ИСО/МЭК, серию X.608 МСЭ‑ Т | серию 14476 ИСО/МЭК, X.602 МСЭ-Т | 16513 ИСО/МЭК, серию X.603 МСЭ-Т | серию 16512 ИСО/МЭК, серию X.604 МСЭ-Т | серию 24793 ИСО/МЭК, X.605 МСЭ-Т | 13252 ИСО/МЭК. Потребуется постоянное поддержание и ведение Рекомендаций, и они могут обновляться в случае возникновения дальнейших требований рынка в будущем.

Различные распределенные и диалоговые мультимедийные услуги, такие как IPTV, цифровой информационный экран, VoD, дистанционное присутствие, услуга персонального радиовещания, потоковая мультимедийная передача и другие появляющиеся услуги доставки контента, требуют обеспечения эффективной возможности связи в различных сетевых средах и должны поддерживать расширенный контент, такой как AR/VR, UHD (4K, 8K). Создание протоколов организаций сетей распределенных услуг на основе одноранговых (P2P) технологий может оказаться одним из полезных решений для обеспечения новых появляющихся приложений, для которых требуются высокие качественные характеристики и возможность расширения связи. ИК11 разрабатывает Рекомендации по архитектуре сигнализации и протоколам для управляемой связи P2P (MP2P), которые могут применяться для сквозной мультимедийной связи, включая услуги потоковой передачи видео и распространения контента. Также была начата и будет продолжена разработка стандартов протоколов для системы гибридной связи P2P (HP2P), состоящей из ячеистой сети P2P и древовидной сети P2P. Протоколы связи HP2P обеспечат возможность эффективного и гибкого распределения информации для услуг, связанных с IoT, и услуг на основе технологии распределенного реестра. Набор разрабатываемых Рекомендаций предложит решения и руководящие указания для производителей и поставщиков, желающих внедрить и развернуть услуги по распределению и доставке разнообразного контента с использованием технологий P2P.

Также во многих ОРС продолжается изучение информационно-ориентированной сети (ICN), в частности, в рамках группы исследования информационно-ориентированных сетей IETF. Рассматриваются вопросы интеграции технологий ICN в существующий интернет путем развертывания наложенных сетей (ICN по протоколу IP), нижележащих сетей (острова ICN внутри IP) или использования ICN в виртуализированной IP-инфраструктуре. Эти подходы описаны в RFC 8763. Протоколы и механизмы обнаружения, распределения и доставки контента, основанные на использовании технологии информационно-ориентированной сети (ICN) при развертывании наложенных сетей, нижележащих сетей и виртуализированной IP-инфраструктуры, явятся очень важными появляющимися вопросами для обеспечения соответствующих требований и возможностей сетей IMT‑2020 и дальнейших поколений.

Рекомендации, относящиеся к сфере охвата данного Вопроса: X.601, X.602, X.603, X.603.1, X.603.2, X.604, X.604.1, X.604.2, X.605, X.606, X.606.1, X.607, X.607.1, X.608 и X.608.1, X.609, X.609.1, X.609.2, X.609.3, X.609.4, X.609.5, X.609.6, X.609.7, X.609.8, X.609.9, X.609.10, Q.4100–Q.4139 (для протоколов и сигнализации P2P-связи).

### Н.2 Вопрос

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

– Как необходимо вести или совершенствовать существующие Рекомендации в ответ на новые требования рынка?

– Какие Рекомендации необходимо разработать для обеспечения протоколов для обнаружения, распределения и доставки контента в целях поддержки требований и функциональных архитектур традиционных сетей, будущих сетей и сетей IMT‑2020 и дальнейших поколений?

– Какие Рекомендации необходимо разработать для обеспечения протоколов для обнаружения, распределения и доставки контента на основе использования технологий ICN при развертывании наложенных сетей, нижележащих сетей и виртуализированной IP‑инфраструктуры, которые учитываются в будущих сетях и сетях IMT‑2020 и дальнейших поколений?

– Какие протоколы и механизмы необходимо разработать для поддержки управляемой и гибридной одноранговой связи?

– Какие механизмы и основные технологии необходимо определить, чтобы реализовать функции, определяемые приложением и информацией из сети?

− Какие интерфейсы и параметры 4-го уровня необходимо определить для верхнего и нижнего уровней соответственно?

### Н.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– ведение и совершенствование Рекомендаций серии X.60x, включая общие с ПК6 ОТК1 ИСО/МЭК тексты стандартов для многосторонней связи, в ответ на новые требования рынка;

– разработка Рекомендаций по протоколам для поддержки обнаружения, распространения и доставки контента для традиционных сетей, будущих сетей и сетей IMT-2020 и дальнейших поколений;

– разработка Рекомендаций по протоколам для поддержки обнаружения, распространения и доставки контента на основе использования технологии информационно-ориентированных сетей (ICN) при развертывании наложенных сетей, нижележащих сетей и виртуализированной IP-инфраструктуры, которые учитываются в сетях IMT-2020 и дальнейших поколений;

– разработка Рекомендаций по протоколам и механизмам для поддержки управляемой и гибридной одноранговой связи;

− разработка Рекомендаций по протоколам для поддержки сквозной многосторонней мультимедийной связи, включая услуги и приложения персонального радиовещания.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?Q=8/11>.

### Н.4 Относящиеся к Вопросу

Рекомендации:

– Рекомендации серии X по многосторонней мультимедийной связи

– Рекомендации серии Y и Добавления по IPTV, доставке контента, DSN, будущим сетям и сетям IMT‑2020 и дальнейших поколений

– Рекомендации серии H по мультимедийным услугам и приложениям

– Рекомендации серии Q по сигнализации, протоколам, измерениям и спецификациям тестирования, относящиеся к данному Вопросу

Вопросы:

− Все вопросы ИК11

Исследовательские комиссии:

– ИК13 МСЭ‑T, ответственная за будущие сети и сети IMT-2020 и дальнейших поколений

– ИК16 МСЭ‑T, ответственная за мультимедийные услуги и приложения

− ИК17 МСЭ‑T, ответственная за соответствующие вопросы безопасности

Другие органы:

– ПК6 ОТК1 ИСО/МЭК

– IETF, ICNRG

Направления деятельности ВВУИО:

– C2

Цели в области устойчивого развития:

– 9

Вопрос I/11

Тестирование интернета вещей, его приложений и систем идентификации

(Продолжение Вопроса 12/11)

### I.1 Обоснование

В широком смысле интернет вещей (IoT) можно воспринимать как концепцию, имеющую технологические и социальные последствия. В отношении технической стандартизации IoT можно рассматривать как глобальную инфраструктуру для информационного общества, обеспечивающую современные услуги путем присоединения (физического и виртуального) вещей на основе существующих и развивающихся, функционально совместимых информационно-коммуникационных технологий. Благодаря использованию возможностей идентификации, сбора данных, обработки и связи, IoT в полной мере использует вещи, чтобы предлагать услуги для всех типов приложений, обеспечивая при этом необходимую конфиденциальность. Понятия "повсеместно распространенное общество", "повсеместно распространенная сеть", "повсеместно распространенный город" и другие были сформулированы в поддержку общемировой сферы распространения приложений, услуг и технологий IoT, которые могут быть обеспечены радиочастотной идентификацией (RFID), повсеместно распространенной сенсорной сетью (ПРСС), машинно-ориентированной связью (MOC), межмашинной (M2M) связью, связью "умных" устройств (SDC), услугами IoT, поддерживающими облачные вычисления (CIS), при этом RFID учитывалась ПК31 ОТК1 ИСО/МЭК, технологии сенсорной сети – РГ7 ОТК1 ИСО/МЭК, ПРСС – ИК20 МСЭ-T, MOC – ИК13 МСЭ-T, M2M – МСЭ-T и ЕТСИ, SDC – TIA, CIS – ЕТСИ, OGC и W3C.

ПРИМЕЧАНИЕ 1. – Термин "повсеместно распространенный" ("u") толкуется как возможность предоставления любых услуг в любое время и в любом месте с помощью любых устройств.

Все эти ключевые слова имеют определенные аналогичные случаи использования и предполагают определенные идентичные функции, но предусматривают некоторые различные технологические взгляды. IoT может рассматриваться как общее понятие для всех этих технологических ключевых слов.

Поскольку IoT представляет собой столь широкую концепцию и может быть связан с различными опорными технологиями, необходимо рассмотреть вопросы функциональной совместимости.

В целом IoT открывает различные новые типы установления соединений, которые могут использоваться в различных ориентированных на потребителей приложениях (например, воздушные повсеместно распространенные сенсорные сети (FUSN), дополненная реальность (AR) на базе IoT и т. д.).

Кроме того, принимая во внимание защищенный механизм аутентификации, используемый в технологиях на базе IoT, и идентичность IoT, интернет вещей можно рассматривать в качестве одного из инструментов, которые следует использовать для борьбы с контрафакцией.

С учетом всего отмеченного выше, в настоящее время тестирование технологий/приложений IoT становится все более важным, особенно с точки зрения функциональной совместимости устройств IoT и доверия к используемым системам IoT.

Помимо традиционных приложений IoT, целесообразно рассмотреть возможность тестирования в тех областях, где происходит наиболее массовое внедрение устройств IoT:

– "умные" устойчивые города;

– носимые устройства;

– промышленный интернет вещей (IIoT);

– сетевые системы помощи при вождении для автономных транспортных средств;

– летающие сети на базе беспилотных летательных аппаратов.

Как правило, в каждой из этих областей имеются разные сценарии подключения устройств IoT к интернету, облачным платформам и удаленным услугам. В этой связи рассмотрение вопросов по процедурам тестирования устройств IoT представляется весьма актуальным.

### I.2 Вопрос

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

− Какие типы тестов требуются для сетевых элементов IoT?

− Как проверить безопасность устройства IoT с учетом его параметров (пропускной способности, объема памяти, канала связи и т. д.)?

− Какие необходимо разработать наборы тестов для тестирования процедур идентификации/аутентификации IoT?

− Как тестировать технические решения IoT, предназначенные для использования для борьбы с контрафакцией?

− Какие новые Рекомендации необходимо разработать для обеспечения механизмов тестирования приложений IoT, включая аспекты безопасности и конфиденциальности?

– Какие новые Рекомендации необходимо разработать для обеспечения механизмов тестирования функциональной совместимости, функциональных возможностей и безопасности систем идентификации IoT?

− Какие сценарии тестирования следует использовать для тестирования носимых устройств?

– Какие сценарии тестирования следует использовать для тестирования системы и устройств промышленного интернета вещей (IIoT)?

– Какие наборы тестов необходимо разработать для проверки методики и/или механизма (процедур) тестирования технологий и протоколов IoT и IIoT на основе прогностического анализа?

– Какие новые Рекомендации необходимо разработать для обеспечения функциональной совместимости (возможности взаимодействия), совместимости и безопасности устройств IoT, предназначенных для "умного" устойчивого города?

– Какие процедуры тестирования необходимо разработать для технологий на базе интернета вещей и протоколов сетевой системы помощи при вождении для автономных транспортных средств?

### I.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– разработка наборов тестов для использования при тестировании сетевых элементов IoT;

− разработка методики тестирования безопасности и спецификации тестов, относящихся к тестированию безопасности IoT;

– разработка наборов тестов для тестирования процедур идентификации/аутентификации IoT;

− разработка наборов тестов для тестирования технических решений IoT, предназначенных для использования для борьбы с контрафакцией;

− разработка методики и/или механизма для тестирования приложений IoT, включая аспекты безопасности и конфиденциальности;

– разработка методики и/или механизма для тестирования функциональной совместимости, функциональных возможностей и безопасности систем идентификации IoT;

− разработка методики и/или механизма тестирования носимых устройств;

– разработка методики и/или механизма тестирования промышленного интернета вещей и приложений IIoT;

– разработка методики и/или механизма тестирования технологий и протоколов IoT и IIoT на основе прогностического анализа;

– разработка методики и/или механизма тестирования технологий на основе интернета вещей и протоколов, предназначенных для "умного" устойчивого города;

– разработка методики и/или механизма тестирования технологий на основе интернета вещей и протоколов сетевой системы помощи при вождении для автономных транспортных средств.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### I.4 Относящиеся к Вопросу

Рекомендации:

− Серии Q, Y, H, I, M и F

Вопросы:

– Вопросы L/11, M/11

Исследовательские комиссии:

− ИК2 МСЭ-T

− ИК5 МСЭ-T

− ИК13 МСЭ-T

− ИК16 МСЭ-T

− ИК17 МСЭ-T

− ИК20 МСЭ-T

Другие органы:

– ЕТСИ, в особенности Технический комитет по кибербезопасности

– IEEE

– IETF

– ОТК1 ИСО/МЭК (в особенности ТК27 ОТК1 ИСО/МЭК, РГ7 ОТК1 ИСО/МЭК, ПК6 ОТК1 ИСО/МЭК, ПК31 ОТК1 ИСО/МЭК, РГ10 ОТК1 ИСО/МЭК)

– OGC

– TIA

– W3C

Направления деятельности ВВУИО:

– C5

Цели в области устойчивого развития:

– 9

Вопрос J/11

Контроль параметров для протоколов, используемых в появляющихся сетях, включая облачные/периферийные вычисления и организацию сетей с программируемыми параметрами/виртуализацию   
сетевых функций (SDN/NFV)

(Продолжение Вопроса 13/11)

### J.1 Обоснование

Были определены и разработаны следующие появляющиеся сети: будущие сети, интернет вещей (IoT), сети на базе VoLTE/ViLTE, сети IMT-2020 и дальнейших поколений и др. В целях сокращения инвестиций и эксплуатационных затрат в появляющихся сетях развернуты сети с программируемыми параметрами (SDN), а также внедряется виртуализация сетевых функций (NFV), с тем чтобы обеспечить разделение управления и услуг, управления и канала-носителя, аппаратного и программного обеспечения.

Кроме того, облачные и периферийные вычисления становятся инфраструктурой кибермира. В этой новой появляющейся среде у операторов и конечных пользователей должны иметься возможности для контролирования того, чтобы используемая ими инфраструктура могла поддерживать такие приложения и услуги.

По мере того как технология ИИ становится все более развитой, она применяется в сетях операторов и интернет-предприятий, например, для интеллектуального принятия решений и интеллектуального прогнозирования. Выбор контролируемых параметров в модели интеллектуального принятия решений или интеллектуального прогнозирования в значительной степени влияет на эффективность сети и в конечном итоге – на взаимодействие с пользователями.

Стандартизация параметров системы контроля появляющихся сетей, включая облачные вычисления, предоставит операторам, администрациям и конечным пользователям информацию о контроле, совместимую и сопоставимую среди различных операторов сетей, поставщиков услуг и конечных пользователей. Кроме того, она может быть полезной при урегулировании разногласий.

### J.2 Вопрос

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

– Каким является минимальный набор параметров, которые необходимо использовать для оценки рабочих характеристик сети?

– Каким является минимальный набор параметров, которые необходимо использовать для контроля облачных вычислений и периферийных вычислений?

– Каким является минимальный набор параметров, которые необходимо использовать для контроля NFV и SDN?

– Каким является минимальный набор параметров, которые необходимо использовать для контроля появляющихся сетей, приложений и услуг?

– Параметры какого вида необходимо использовать для контроля вопросов безопасности?

− Какие параметры необходимо использовать для применения технологии искусственного интеллекта в появляющихся сетях, приложениях и услугах?

− Каким является минимальный набор параметров, которые необходимо использовать для контроля интеллектуальных сетей, приложений и услуг?

### J.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– разработка минимального набора и методики измерения параметров, которые необходимо использовать для оценки рабочих характеристик сети;

– разработка минимального набора и методики измерения параметров, которые необходимо использовать для оценки облачных вычислений и периферийных вычислений;

– разработка минимального набора и методики измерения параметров, которые необходимо использовать для оценки NFV и SDN;

– разработка минимального набора и методики измерения параметров, которые необходимо использовать для оценки появляющихся сетей, приложений и услуг;

– изучение того, параметры какого вида необходимо использовать для контроля вопросов безопасности;

− изучение видов параметров, которые необходимо использовать для применения технологии искусственного интеллекта в появляющихся сетях, приложениях и услугах;

− изучение видов параметров, которые необходимо использовать для контроля интеллектуальных сетей, приложений и услуг.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### J.4 Относящиеся к Вопросу

Рекомендации:

− Серии Q, Y, H, I, M, F и Р МСЭ-T

Вопросы:

– Вопросы A/11, B/11, D/11, G/11, I/11, K/11 и M/11

Исследовательские комиссии:

– ИК3 МСЭ‑T, ответственная за вопросы политики и регулирования

– ИК12 МСЭ‑T, ответственная за вопросы, связанные с QoS/QoE

– ИК13 МСЭ‑T, ответственная за будущие сети, SDN/NFV, облачные вычисления и архитектуру появляющихся сетей

– ИК16 МСЭ‑T, ответственная за мультимедийные услуги и приложения

– ИК17 МСЭ-Т, ответственная за вопросы безопасности

– ИК20 МСЭ-Т, ответственная за IoT и его приложения

Другие органы:

– ЕТСИ

– IEEE

– IETF

Направления деятельности ВВУИО:

– C2, C5

Цели в области устойчивого развития:

– 9

Вопрос K/11

Тестирование облачных вычислений, SDN и NFV

(Продолжение Вопроса 14/11)

### K.1 Обоснование

Облачные вычисления –это парадигма обеспечения сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу. Сети с программируемыми параметрами – это набор методов, которые позволяют напрямую программировать, организовывать, контролировать сетевые ресурсы и управлять ими, что облегчает проектирование, доставку и эксплуатацию сетевых услуг динамичным и масштабируемым образом. Виртуализация сетевых функций – это принцип отделения сетевых функций от аппаратного обеспечения, на котором они работают, с помощью абстрагирования виртуального аппаратного обеспечения.

Облачные вычисления, SDN и NFV – это появляющиеся технологии, широко используемые в различных сценариях. Соответствие, функциональная совместимость и оценочное тестирование облачных вычислений, SDN и NFV – чрезвычайно важные для изучения темы.

В контексте облачных вычислений/SDN/NFV проверка согласования – это тестирование для проверки того, что реализация облачных вычислений/SDN/NFV соответствует разработанному стандарту, например стандарту функциональных требований или спецификации протокола. Проверка на функциональную совместимость – это тестирование для оценки способности объектов, вовлеченных в облачные вычисления/SDN/NFV, взаимодействовать друг с другом ожидаемым образом. Оценочное тестирование используется для оценки реализации облачных вычислений/SDN/NFV с точки зрения рабочих характеристик.

Кроме того, с использованием технологий облачных вычислений, SDN и NFV, таких как SD-WAN, реализуется все больше и больше услуг. Необходимо рассмотреть возможность тестирования услуг на основе облачных вычислений, SDN и NFV.

Необходимо сотрудничество с ИК13 МСЭ-T (ведущей ИК по облачным вычислениям) в области тестирования облачных вычислений. Проведение тестирования, связанного с облачными вычислениями, начнется после того, как ИК13 определит терминологию и архитектуру.

### K.2 Вопрос

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

– Каковы требования к соответствию, функциональной совместимости и оценочному тестированию облачных вычислений, SDN и NFV?

– Какие наборы тестов необходимы для тестирования облачных вычислений, SDN и NFV, включая аспект соответствия, функциональной совместимости и оценочного тестирования?

– Как создать автоматизированную систему тестирования облачных вычислений, SDN и NFV для повышения эффективности тестирования?

– Какие наборы тестов необходимы для тестирования услуг, реализуемых средствами облачных вычислений, SDN и NFV?

– Какое требуется сотрудничество для максимального сокращения дублирования работы с другими ОРС?

– Какое требуется сотрудничество для использования сообщества разработчиков программного обеспечения с открытым исходным кодом?

### K.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– определение требований к соответствию, функциональной совместимости и оценочному тестированию облачных вычислений, SDN и NFV;

– разработка наборов тестов для тестирования соответствия, функциональной совместимости и оценочного тестирования облачных вычислений, SDN и NFV;

– разработка методики и структуры автоматизированного тестирования облачных вычислений, SDN и NFV;

– разработка наборов тестов для тестирования услуг, реализуемых средствами облачных вычислений, SDN и NFV;

– обеспечение необходимого сотрудничества с внешними ОРС, консорциумами и форумами, а также сообществами разработчиков программного обеспечения с открытым исходным кодом;

– ведение и совершенствование Рекомендаций, которые входят в сферу охвата данного Вопроса.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### K.4 Относящиеся к Вопросу

Рекомендации:

− Серии Q, Y, H, I, M и F (в особенности Рекомендации, касающиеся облачных вычислений и тестирования)

Вопросы:

– Все Вопросы ИК11

Исследовательские комиссии:

– ИК2, ответственная за эксплуатационные аспекты

– ИК12, ответственная за QoS/QoE

– ИК13, ответственная за архитектуру будущих сетей и облачные вычисления

− ИК15, ответственная за транспортирование, доступ и жилища

– ИК16, ответственная за мультимедийные услуги и приложения

– ИК17, ответственная за безопасность

Другие органы:

– ОТК1 ИСО/МЭК (в особенности ПК38 ОТК1 ИСО/МЭК)

– IETF

– NFV ISG ЕТСИ

– IEEE

– OASIS

– NIST

– Форум TM

− ONF

Направления деятельности ВВУИО:

– C2, C5, C11

Цели в области устойчивого развития:

– 9

Вопрос L/11

Борьба с использованием контрафактных и похищенных устройств электросвязи/ИКТ

(Продолжение Вопроса 15/11)

### L.1 Обоснование

Работа в рамках этого Вопроса была в основном сосредоточена на разработке Рекомендаций и Технических отчетов по борьбе с контрафактными устройствами электросвязи/ИКТ. Растущее использование оборудования электросвязи/ИКТ в повседневной жизни людей в последние годы привело к увеличению проблем, связанных с продажей, обращением и использованием контрафактных устройств на большинстве рынков, а также с их отрицательными последствиями для производителей, пользователей и правительств.

Было обнаружено, что значительная часть устройств электросвязи/ИКТ являются контрафактными и создают проблемы, связанные с национальной безопасностью, показателями работы, качеством предоставляемых услуг и потерей доходов для всех заинтересованных сторон. Это привело к тому, что Государства − Члены МСЭ, в частности развивающиеся страны, обратились с призывом рассмотреть этот вопрос, в особенности негативное влияние, и изучить любое положительное воздействие принятых мер.

Кроме того, спрос на услуги, приводящий к росту производства и наличия устройств электросвязи/ИКТ, также сопровождался увеличением числа похищенных устройств. Часть этих устройств возвращается на рынок после взлома и изменения идентификационных номеров, в результате чего удается обойти внедряемые правительствами и операторами сетей подвижной связи решения по составлению черных списков идентификационных номеров. В связи с этим большинство стран мира не только вовлечены в борьбу с контрафактными устройствами электросвязи/ИКТ, но и внедрили меры, направленные против хищения устройств электросвязи/ИКТ, в том числе позволяющие обеспечить блокировку повторной активации в сетях похищенных устройств с измененными идентификационными номерами и эффективное управление такой ситуацией.

ИК11 утвердила Рекомендацию МСЭ-T Q.5050 "Концептуальное решение по борьбе с контрафактными устройствами ИКТ", Рекомендацию МСЭ-Т Q.5051 "Принципы борьбы с использованием похищенных мобильных устройств" и приступила к работе по ряду новых направлений.

В МСЭ и повсюду в мире обсуждается вопрос о том, могут ли программы по оценке соответствия и проверке на функциональную совместимость стать одним из решений для борьбы с контрафактными устройствами ИКТ. В Резолюции 188 (Пересм. Дубай, 2018 г.) Полномочной конференции МСЭ признается, что подделка устройств электросвязи/ИКТ может снизить эффективность решений, принимаемых странами для борьбы с контрафактной продукцией, и предлагается Государствам-Членам принять все необходимые меры для борьбы с контрафактными устройствами электросвязи/ИКТ. Любые уникальные и стойкие идентификаторы могут позволить определять подлинные продукты. Кроме того, особое внимание следует уделять потенциальному росту числа контрафактных устройств IoT и его возможным последствиям.

Кроме того, в Резолюции 189 (Пересм. Дубай, 2018 г.) Полномочной конференции МСЭ о борьбе с хищениями мобильных устройств решено изучить этот вопрос и поощрять разработку способов и средств продолжения борьбы с хищением мобильных устройств и предотвращения этого явления, а Государствам-Членам предлагается принять необходимые меры по предотвращению, обнаружению и контролю подделки и репликации идентификаторов мобильных устройств ИКТ, а также предотвращению доступа этих устройств в сети подвижной связи.

Данный Вопрос направлен на изучение соответствующих возможностей по решению проблемы борьбы с использованием похищенных и контрафактных устройств электросвязи/ИКТ и, в частности, на ее связь с управлением определением идентичности в цепочке поставки продуктов, с отслеживанием, безопасностью, конфиденциальностью, доверием людей и сетями. Для сбора всей информации и понимания этого вопроса, в том числе для организации в сотрудничестве со всеми заинтересованными сторонами семинара/практикума, потребуется сотрудничество между исследовательскими комиссиями МСЭ-T, между МСЭ-T и МСЭ-D, а также с внешними органами, не входящими в МСЭ (в частности, с ОРС). Для выполнения этих задач также необходима координация деятельности соответствующих организаций.

В рамках этого Вопроса будет осуществляться ведение Рекомендаций МСЭ-T Q.5050−Q.5069 и технических отчетов МСЭ-T TR-CF.

### L.2 Вопрос

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

– Какие Технические отчеты необходимы для повышения уровня осведомленности о проблеме контрафактных устройств ИКТ и об опасностях, которые они представляют?

– Могут ли системы проверки на соответствие и функциональную совместимость и системы их оценки использоваться для борьбы с контрафактным оборудованием электросвязи/ИКТ?

– Какие технологии могут использоваться в качестве инструмента борьбы с контрафактными, поддельными и похищенными устройствами электросвязи/ИКТ?

– Какие структуры управления определением идентичности подходят для борьбы с контрафактными и похищенными устройствами электросвязи/ИКТ с измененными идентификационными номерами?

– Какие новые категории устройств электросвязи/ИКТ следует рассматривать как контрафактные и какой подходящий уникальный идентификатор устройства следует принять для каждой категории?

– Какого вида Рекомендации, Добавления, Технические отчеты и Руководящие указания следует разработать для борьбы с контрафакцией ИКТ, подделкой, изменением и/или дублированием уникальных идентификаторов устройств и для выработки соответствующих решений?

– Какого вида Рекомендации, Добавления, Технические отчеты и Руководящие указания следует разработать для содействия Членам МСЭ в борьбе, в сотрудничестве с Сектором МСЭ-D, с контрафакцией и в ограничении использования похищенных устройств ИКТ?

– Какие Рекомендации, Добавления, Технические отчеты и Руководящие указания МСЭ требуются для безопасного управления цепочкой поставок (от производства до ввоза, распределения и сбыта), чтобы улучшить отслеживание, безопасность продуктов и сетей, защиту конфиденциальной информации и укрепить доверие людей?

– Какие Рекомендации, Добавления, Технические отчеты и Руководящие указания МСЭ подходят для борьбы с контрафакцией устройств IoT и решения проблем, которые она может вызвать?

– Что следует учитывать в этом направлении для прямого или косвенного обеспечения экономии энергии в отрасли ИКТ или других отраслях?

### L.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– разработка Рекомендаций, Добавлений, Технических отчетов и Руководящих указаний для содействия Членам МСЭ в борьбе, в сотрудничестве с Сектором МСЭ-D, с контрафакцией устройств электросвязи/ИКТ и решении проблем, которые она может вызвать;

– разработка Рекомендаций, Добавлений, Технических отчетов и Руководящих указаний для содействия Членам МСЭ в борьбе, в сотрудничестве с Сектором МСЭ-D, с контрафакцией устройств IoT;

– разработка Рекомендаций, Добавлений, Технических отчетов и Руководящих указаний для решения проблемы похищенных устройств электросвязи/ИКТ и для содействия Членам МСЭ по внедрению, в сотрудничестве с Сектором МСЭ-D, решений для сокращения масштабов использования похищенных устройств;

– разработка Рекомендаций, Добавлений, Технических отчетов и Руководящих указаний для определения новых категорий устройств электросвязи/ИКТ, которые могут выиграть от борьбы с контрафакцией, а также для определения типов идентификаторов устройств, которые следует рассмотреть для каждой категории;

– изучение соответствующих решений, включая структуры управления определением идентичности, для борьбы с контрафактными и похищенными устройствами электросвязи/ИКТ с поддельными или дублированными уникальными идентификаторами;

– изучение соответствующих технологий, которые могут использоваться в качестве инструмента борьбы с распространением контрафактных, поддельных и похищенных устройств электросвязи/ИКТ и с его опасными последствиями;

– организация, в сотрудничестве с Сектором МСЭ-D, во всех регионах МСЭ семинаров-практикумов и мероприятий для пропагандирования работы МСЭ-Т в этой области и привлечения заинтересованных сторон;

– изучение возможных решений в области проверки на соответствие и функциональную совместимость (C&I) для борьбы с контрафакцией и подделкой устройств электросвязи/ИКТ, принимая во внимание деятельность Руководящего комитета МСЭ-Т по оценке соответствия (CASC);

– изучение результатов, достигнутых различными международными органами по стандартизации, и разработка технических спецификаций для пополнения проводимой в рамках Вопроса работы по стандартизации.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### L.4 Относящиеся к Вопросу

Резолюции:

– Резолюция 188 (Пересм. Дубай, 2018 г.) Полномочной конференции "Борьба с контрафактными устройствами электросвязи/информационно-коммуникационных технологий"

– Резолюция 189 (Пересм. Дубай, 2018 г.) Полномочной конференции "Оказание Государствам‑Членам помощи в борьбе с хищениями мобильных устройств и в предотвращении этого явления"

– Резолюция 79 (Пересм. Буэнос-Айрес, 2017 г.) ВКРЭ "Роль электросвязи/информационно-коммуникационных технологий в борьбе с контрафактными устройствами электросвязи/информационно-коммуникационных технологий и в решении этой проблемы"

– Резолюция 76 (Пересм. Хаммамет, 2016 г.) ВАСЭ "Исследования, касающиеся проверки на соответствие и функциональную совместимость, помощи развивающимся странам и возможной будущей программы, связанной со Знаком МСЭ"

− Резолюция 96 (Пересм. Хаммамет, 2016 г.) ВАСЭ "Исследования Сектора стандартизации электросвязи МСЭ в области борьбы с контрафактными устройствами электросвязи/информационно-коммуникационных технологий"

– Резолюция 97 (Пересм. Хаммамет, 2016 г.) ВАСЭ "Борьба с хищениями мобильных устройств электросвязи"

Рекомендации:

− МСЭ-T X.1255, МСЭ-T X.660, МСЭ-T Q.5050, МСЭ-T Q.5051

Вопросы:

– Все вопросы ИК11, особенно Вопросы, касающиеся управления, архитектуры сигнализации, протоколов, проверки на соответствие и функциональную совместимость

Исследовательские комиссии:

– ИК2 МСЭ-T

− ИК3 МСЭ-T

− ИК5 МСЭ-T

− ИК12 МСЭ-T

− ИК13 МСЭ-T

− ИК17 МСЭ-T

− ИК20 МСЭ-T

− ИК1 и ИК2 МСЭ-D

Другие органы:

– ЕТСИ

– МЭК

– IEEE

– IETF

– ОТК1 ИСО/МЭК

Направления деятельности ВВУИО:

– C2, C5, C11

Цели в области устойчивого развития:

– 9

Вопрос M/11

Спецификации тестирования протоколов, сетей и услуг для появляющихся технологий, включая оценочное тестирование

(Продолжение Вопроса 16/11)

### M.1 Обоснование

В Резолюции 76 ВАСЭ "Исследования, касающиеся проверки на соответствие и функциональную совместимость, помощи развивающимся странам и возможной будущей программы, связанной со Знаком МСЭ" в разделе *решает* говорится, что 11-я Исследовательская комиссия МСЭ-T координирует деятельность Сектора, касающуюся программы МСЭ в области соответствия и функциональной совместимости (C&I), во всех исследовательских комиссиях и рассматривает рекомендации, содержащиеся в бизнес-плане C&I, для долгосрочного осуществления программы C&I.

МСЭ-T выпускает большое число Рекомендаций. Для обеспечения соответствия и функциональной совместимости один из важных аспектов программы C&I МСЭ связан с разработкой и поддержанием структур и методик тестирования.

Очень важно, чтобы методики проверки на соответствие и функциональную совместимость, используемые всеми исследовательскими комиссиями, которые участвуют в тестировании, были согласованы и соответствовали друг другу. Для достижения функциональной совместимости в глобальном масштабе Рекомендации МСЭ-Т должны разрабатываться и поддерживаться с учетом соответствия и функциональной совместимости согласно надлежащей методике.

При проверке на соответствие задача состоит в том, чтобы определить, насколько полно и точно в реализации выполнены требования, указанные в Рекомендации. Напротив, при проверке на функциональную совместимость задача состоит в том, чтобы определить, взаимодействуют ли две или более реализаций одной и той же Рекомендации и правильно ли они обмениваются информацией между собой. Обычно считается, что та или иная реализация протестирована на соответствие, прежде чем осуществляется оценка, связанная с проверкой на функциональную совместимость.

Последние тенденции (такие, как технологии IMT-2020, IoT) могут инициировать многочисленные изменения в существующей сетевой архитектуре, что предусматривает необходимость обеспечения более высокой производительности сети. Это, в свою очередь, повлияет на характеристики оконечных устройств, таких как CPE, мобильные устройства, телефоны и т. д.

Большинство операторов электросвязи внедряют различные появляющиеся технологии и переходят от сетей с коммутацией каналов на сети с коммутацией пакетов, стараясь предоставлять свои услуги с использованием концепции "все по IP". В результате операторы сталкиваются с рядом проблем, которые в целом связаны с совместимостью, в том числе функциональной, используемого оборудования ИКТ и присоединением сетей на базе IP (например, 4G, IMT-2020), которые, в числе прочих, будут использоваться для услуг роуминга/кочевой связи. Например, предоставление услуг роуминга голоса и изображений по LTE (VoLTE/ViLTE) создает для операторов некоторые проблемы ввиду отсутствия согласованных между заинтересованными сторонами процедур роуминга, различных имеющихся сценариев реализации VoLTE/ViLTE и других нестандартизированных вопросов (например, ENUM, экстренный вызов и др.). Проверка на соответствие и функциональную совместимость интерфейсов сеть-сеть (NNI) в сравнении с Рекомендацией МСЭ-Т может помочь операторам удостовериться в том, что их решения VoLTE/ViLTE готовы для присоединения. Такой подход к присоединению может использоваться также для будущих сетей на основе пакетов, например сетей IMT-2020 и дальнейших поколений.

В большинстве случаев сравнительный анализ является общепринятым подходом, который используется для измерения и тестирования параметров сигнализации в сравнении с проектными параметрами показателей работы, что должно помочь в обеспечении сквозной доставки услуг и надежности сети.

Применительно к IMT-2020 сравнительный анализ не ограничивается только транспортным уровнем и включает показатели работы, качество и надежность виртуальных платформ.

Важным вопросом для операторов и пользователей является определение значений показателей работы сети и продуктивности услуг с требуемым качеством обслуживания (QoS).

Например, системы измерений связанных с интернетом показателей работы, которые общедоступны в интернете, не обеспечивают надежных и сопоставимых измерений. Помимо отсутствия в Рекомендациях МСЭ-Т стандартизированных параметров скорости интернет-соединения, полученные тестовые результаты, которых можно добиться с использованием существующего метода тестирования, могут отличаться от результатов, полученных с помощью других методов. Несомненно, результаты тестирования зависят от сегментов сети, которые используются при соединении e2e. В частности, невозможно гарантировать, что соединение e2e основано только на сети оператора электросвязи и не включает другие сетевые сегменты, которые могут принадлежать другим операторам.

Разработка единого подхода к измерению связанных с интернетом показателей работы важна для всех участников отрасли ИКТ.

Кроме того, такой стандартизированный подход будет содействовать разработке "*основы для предоставления услуг ИКТ с гарантированным QoS и требуемой скоростью передачи в сетях фиксированной и подвижной передачи данных для разработки эффективных экономических механизмов и моделей взаимодействия по линии оператор-поставщик-пользователь*".

ПРИМЕЧАНИЕ. – Показатели работы сети, QoS/QoE, в том числе KPI, параметры сетей и услуг и требования к ним, определяются ИК12 МСЭ‑T и соответствующими ОРС. В сферу ответственности данного Вопроса входят серия Q.3900−Q.4099 (тестирование для сетей последующих поколений), серия Q.1912.x, серия X.290 (за исключением X.292), X.Доб.4, X.Доб.5 и серия Z.500.

### M.2 Вопрос

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

– Какова методика тестирования появляющихся технологий?

– Какие существуют Рекомендации МСЭ‑Т, включающие комплекты тестов?

– Какую архитектуру испытательного стенда или средств тестирования следует использовать для тестирования появляющихся технологий?

– Какие разрабатываемые для рынка ИКТ технологии требуют проверки на соответствие и функциональную совместимость (с учетом потребностей рынка)?

– Какие наборы тестов необходимы для тестирования взаимодействия сетей на базе IP (таких, как сети 4G, сети IMT-2020 и дальнейших поколений)?

− Для какого типа оборудования можно проводить оценочное тестирование?

– Какие процедуры тестирования могут быть использованы для оценочного тестирования?

– Какой тип трафика может моделироваться для оценочного тестирования?

– Для каких проектных параметров необходимо проводить оценочное тестирование?

– Какие процедуры тестирования на стандартизированные параметры сети, включая параметры, определенные в структуре измерений показателей работы, связанных с интернетом (МСЭ-T Q.3960), таких как скорость передачи данных e2e внутри и за пределами сети оператора фиксированной и подвижной связи (т. е. сеть между пользователями сети оператора и конкретным интернет-ресурсом), необходимо разработать?

− Каким образом параметры/технологии/услуги могут быть протестированы дистанционно?

– Какие процедуры требуется разработать для внедрения дистанционного тестирования?

– Какая сетевая архитектура должна использоваться для дистанционного тестирования?

– Какова методика тестирования мобильных устройств IMT-2020?

– Для какой методики тестирования услуг требуется сверхмалое время задержки?

### M.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– изучение методики тестирования появляющихся технологий;

– определение существующих Рекомендаций МСЭ‑Т, включающих комплекты тестов;

– определение архитектуры испытательного стенда или средств тестирования, которые следует использовать для тестирования появляющихся технологий;

– определение ориентированных на рынок технологий ИКТ, для которых требуется проверка на соответствие и функциональную совместимость;

– разработка комплектов тестов, которые следует использовать для тестирования взаимодействия IP-сетей (таких, как сети 4G и сети IMT-2020 и дальнейших поколений);

– определение типов оборудования, с которым можно проводить оценочное тестирование;

– разработка процедур оценочного тестирования;

– определение типа трафика, моделируемого для оценочного тестирования;

– определение проектных показателей, по которым необходимо провести оценочное тестирование;

– разработка процедур тестирования стандартизированных параметров сети, в том числе определенных в структуре измерений показателей работы, связанных с интернетом (МСЭ-T Q.3960), таких как скорость передачи данных e2e внутри и за пределами сети оператора фиксированной и подвижной связи (т. е. между пользователями сети оператора и конкретным интернет-ресурсом);

– определение параметров/технологий/услуг, которые могут быть протестированы дистанционно;

– разработка процедур, необходимых для внедрения дистанционного тестирования;

– указание сетевой архитектуры, которая должна использоваться для дистанционного тестирования;

– разработка методики (руководства), которая распространит имеющийся опыт и подходы к тестированию на сети IMT-2020;

– определение методики тестирования устройств IMT-2020;

– определение методики тестирования услуг, для которых требуется сверхмалое время задержки.

Информация о текущем состоянии работы по данному Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### M.4 Относящиеся к Вопросу

Рекомендации:

− Серии Q, Y, H, G, Е, I, M, P, X, Z и F

Вопросы:

– Все Вопросы ИК11 МСЭ‑Т

Исследовательские комиссии:

– ИК13 МСЭ‑T, ответственная за будущие сети (SDN, NFV), облачные вычисления, IMT‑2020, машинное обучение

– ИК15 МСЭ‑T, ответственная за базовые технологии и технологии доступа

– ИК16 МСЭ‑T, ответственная за мультимедийные услуги, приложения и электронное здравоохранение

– ИК17 МСЭ-Т, ответственная за языки тестирования, включая TTCN-3

– Все другие ИК МСЭ-Т, участвующие в деятельности по C&I, сетям IMT-2020 и дальнейших поколений, машинному обучению

– ИК1 и ИК2 МСЭ-D, ответственные за центры дистанционного тестирования

− ИК3 МСЭ‑T, ответственная за вопросы политики

– ИК12 МСЭ‑T, ответственная за параметры QoS и требования к QoS

Другие органы:

– ЕТСИ (в особенности TC INT ЕТСИ и TC NTECH ЕТСИ)

– IETF

– IEEE

Направления деятельности ВВУИО:

– C5, C6

Цели в области устойчивого развития:

– 9

Вопрос N/11

Борьба с контрафактным и поддельным программным обеспечением электросвязи/ИКТ

(Продолжение Вопроса 17/11)

### N.1 Обоснование

В Резолюции 188 (Пересм. Дубай, 2018 г.) Полномочной конференции МСЭ признается вред, причиняемый контрафактными устройствами электросвязи/ИКТ органам государственной власти, производителям, поставщикам и потребителям, утверждается, что подделка устройств электросвязи/ИКТ может снизить эффективность решений, внедряемых странами для борьбы с контрафакцией, и предлагается Государствам-Членам принять все необходимые меры для борьбы с распространением контрафактных устройств электросвязи/ИКТ.

В то же время в Резолюции 96 (Хаммамет, 2016 г.) Всемирной ассамблеи по стандартизации электросвязи признается, что контрафактные и поддельные устройства электросвязи/ИКТ негативно влияют на безопасность и конфиденциальность пользователей и причиняют ущерб органам государственной власти, производителям, поставщикам, операторам и потребителям, например, в виде потери доходов, снижения ценности торговой марки/нарушения прав интеллектуальной собственности, нанесения ущерба репутации и нарушения работы сетей.

Кроме того, в Резолюции 189 (Пересм. Дубай, 2018 г.) Полномочной конференции МСЭ о борьбе с хищениями мобильных устройств признается, что хищение устройств может иметь негативные последствия для данных пользователей и их чувства безопасности и уверенности при применении информационно-коммуникационных технологий (ИКТ), и решено изучить этот вопрос и поощрять разработку способов и средств продолжения борьбы с хищением мобильных устройств и предотвращения этого явления, а Государствам-Членам предлагается принять необходимые меры по предотвращению, обнаружению и контролю подделки и репликации идентификаторов мобильных устройств ИКТ.

В Резолюции 97 (Хаммамет, 2016 г.) Всемирной ассамблеи по стандартизации электросвязи признается, что хищение принадлежащих пользователям мобильных устройств может привести к преступному использованию услуг и приложений электросвязи/ИКТ, что влечет за собой экономический ущерб для законных владельцев и пользователей, и указывается на необходимость определить существующие и будущие технологические меры с применением программных и аппаратных средств для смягчения последствий использования похищенных мобильных устройств.

ИК11 МСЭ-Т получила вклады от Государства – Члена МСЭ и членов Сектора, которые привели к утверждению Рекомендации МСЭ-T Q.5050 "Концептуальное решение по борьбе с контрафактными устройствами ИКТ" и Рекомендации МСЭ-Т Q.5051 "Принципы борьбы с использованием похищенных мобильных устройств". Кроме того, был согласован ряд новых направлений работы.

В то же время в некоторых вкладах говорится о необходимости реагирования на ряд новых сценариев, таких как:

i) подделка программного обеспечения похищенных мобильных устройств в целях получения несанкционированного доступа к данным пользователей с соответствующими последствиями;

ii) контрафактные/поддельные сетевые устройства (такие, как маршрутизаторы или коммутаторы) с лазейками для доступа к сети пользователя, что позволяет похищать данные и чревато потерей доходов;

iii) контрафактные/поддельные ТВ-приемники платного телевидения с поддельным программным обеспечением, которое позволяет лицам, не являющимся абонентами, получить несанкционированный доступ к данным поставщика контента.

Эта проблема не имеет простого решения, поскольку пользователи услуг электросвязи/ИКТ, как правило, не осведомлены об уязвимостях, которые входят в состав контрафактных устройств или могут присутствовать в контрафактном или поддельном программном обеспечении ИКТ. Поэтому крайне важно повышать степень осведомленности всех заинтересованных сторон по этой теме.

Таким образом, данный Вопрос направлен на изучение соответствующих возможностей борьбы с контрафактным или поддельным программным обеспечением ИКТ. Для сбора всей информации и понимания этого вопроса, в том числе для организации в сотрудничестве со всеми заинтересованными сторонами семинара/практикума, потребуется сотрудничество между исследовательскими комиссиями МСЭ-T, между МСЭ-T и МСЭ-D, а также с внешними органами, не входящими в МСЭ (в частности, с ОРС). Для выполнения этих задач также необходима координация деятельности соответствующих организаций.

### N.2 Вопрос

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

– Какой ущерб причиняет заинтересованным сторонам использование контрафактных устройств электросвязи/ИКТ или устройств с поддельным или контрафактным программным обеспечением и последующее незаконное присвоение данных?

– Какой ущерб могут причинить контрафактные устройства электросвязи/ИКТ и/или легитимные устройства с поддельным программным обеспечением заинтересованным сторонам (таким, как пользователи и поставщики услуг), в частности, в результате незаконного присвоения данных?

– Какие Технические отчеты и Руководящие указания необходимы для повышения степени осведомленности о проблемах подделки программного обеспечения электросвязи/ИКТ и незаконного присвоения данных, а также об их последствиях?

– Какие Рекомендации, Добавления, Технические отчеты и Руководящие указания следует разработать для содействия Членам МСЭ в борьбе, в сотрудничестве с Сектором МСЭ-D, с контрафактным и поддельным программным обеспечением электросвязи/ИКТ, незаконным присвоением данных и их последствиями?

– Какие Рекомендации, Технические отчеты и Руководящие указания следует разработать для предотвращения незаконного присвоения данных ИКТ, в частности данных пользователей, содержащихся на устройствах ИКТ, и контента, предоставляемого поставщиками услуг ИКТ?

– Какие технологии и решения могут использоваться для борьбы с контрафактным или поддельным программным обеспечением электросвязи/ИКТ и его вредными последствиями?

– Можно ли использовать схемы оценки соответствия для борьбы с контрафактным или поддельным программным обеспечением ИКТ?

### N.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– исследование ущерба, причиняемого заинтересованным сторонам использованием контрафактных устройств электросвязи/ИКТ или устройств с поддельным или контрафактным программным обеспечением и последующим незаконным присвоением данных;

– изучение соответствующих подходящих технологий и решений, которые можно использовать для борьбы с контрафактным или поддельным программным обеспечением ИКТ, последующим незаконным присвоением данных и другими вредными последствиями;

– разработка Рекомендаций, Добавлений, Технических отчетов и Руководящих указаний для содействия Членам МСЭ в борьбе, в сотрудничестве с Сектором МСЭ-D, с контрафактным и поддельным программным обеспечением ИКТ, незаконным присвоением данных и их вредными последствиями;

– организация, в сотрудничестве с Сектором МСЭ-D, во всех регионах МСЭ семинаров-практикумов и мероприятий для пропагандирования работы МСЭ-Т в этой области и привлечения заинтересованных сторон;

– изучение возможных схем оценки соответствия для борьбы с контрафактным и поддельным программным обеспечением ИКТ и незаконным присвоением данных, принимая во внимание деятельность CASC МСЭ-T;

– изучение результатов, достигнутых различными международными органами по стандартизации, и разработка технических спецификаций для пополнения проводимой в рамках Вопроса работы по стандартизации.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК11 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>.

### N.4 Относящиеся к Вопросу

Резолюции:

– Резолюция 188 (Пересм. Дубай, 2018 г.) Полномочной конференции "Борьба с контрафактными устройствами электросвязи/информационно-коммуникационных технологий"

– Резолюция 189 (Пересм. Дубай, 2018 г.) Полномочной конференции "Оказание Государствам-Членам помощи в борьбе с хищениями мобильных устройств и в предотвращении этого явления"

− Резолюция 96 (Пересм. Хаммамет, 2016 г.) ВАСЭ "Исследования Сектора стандартизации электросвязи МСЭ в области борьбы с контрафактными устройствами электросвязи/информационно-коммуникационных технологий"

– Резолюция 97 (Пересм. Хаммамет, 2016 г.) ВАСЭ "Борьба с хищениями мобильных устройств электросвязи"

Рекомендации:

– МСЭ-T X.1127, МСЭ-T Q.5050, МСЭ-T Q.5051

Вопросы:

– Все Вопросы ИК11, особенно Вопросы, касающиеся управления, архитектуры сигнализации, протоколов, проверки на соответствие и функциональную совместимость, борьбы с контрафактными и похищенными устройствами ИКТ

Исследовательские комиссии:

– ИК2 МСЭ-Т

– ИК3 МСЭ-Т

– ИК9 МСЭ-Т

– ИК13 МСЭ-Т

– ИК16 МСЭ-Т

– ИК17 МСЭ-Т

– ИК20 МСЭ-Т

– ИК1 и ИК2 МСЭ-D

Другие органы:

– ЕТСИ

– МЭК

– IEEE

– IETF

– ОТК1 ИСО/МЭК

Направления деятельности ВВУИО:

– C2, C5, C9, C11

Цели в области устойчивого развития:

– 9

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