|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A logo of a flag  Description automatically generated | Всемирная ассамблея по стандартизации электросвязи (ВАСЭ-24) Нью-Дели, 15−24 октября 2024 года | | | A blue logo with a globe and lightning  Description automatically generated |
|  | | | | |
|  | |  | | |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | | Документ | 10-R | |
|  | | Октябрь 2024 года | | |
|  | | Оригинал: английский | | |
|  | | | | |
| 11-я Исследовательская комиссия МСЭ-Т  Требования к сигнализации, протоколы, спецификации тестирования и борьба с контрафактными устройствами электросвязи/ИКТ | | | | |
| ОТЧЕТ ИК11 МСЭ-Т ВСЕМИРНОЙ АССАМБЛЕЕ ПО СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ (ВАСЭ-24): ЧАСТЬ II – ВОПРОСЫ,  ПРЕДЛАГАЕМЫЕ ДЛЯ ИССЛЕДОВАНИЯ В СЛЕДУЮЩЕМ  ИССЛЕДОВАТЕЛЬСКОМ ПЕРИОДЕ (2025–2028 гг.) | | | | |
|  | | | | |
|  | | | | |

|  |  |  |
| --- | --- | --- |
| **Резюме**: | В настоящем вкладе содержится текст Вопросов 11-й Исследовательской комиссии, предлагаемых для утверждения Ассамблеей на исследовательский период 2025–2028 годов. | |
| **Для контактов**: | г-н Риту Ранджан МИТТАР (Mr Ritu Ranjan MITTAR) Председатель ИК11 МСЭ-T Индия | Тел.: +919868137776 Эл. почта: [rr.mittar@gov.in](mailto:rr.mittar@gov.in) |

Примечание БСЭ

Отчет 11-й Исследовательской комиссии для ВАСЭ-24 представлен в следующих документах:

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

Часть II: **Документ 10** – Вопросы, предлагаемые для исследования в исследовательском периоде 2025–2028 годов

# 1 Перечень 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 с применением появляющихся технологий | 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 пограничного шлюза сети в контексте виртуализации и интеллектуализации сети | Продолжение Вопроса 5/11 |
| F/11 | Протоколы, поддерживающие технологии контроля и управления для сетей Международной подвижной электросвязи | Продолжение Вопроса 6/11 |
| G/11 | Требования к сигнализации и протоколы подсоединения 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 сети, ориентированной на информацию (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 | Мониторинг и измерение 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/периферийных вычислений, SDN и NFV | Продолжение Вопроса 14/11 |
| L/11 | Борьба с использованием контрафактных и похищенных устройств электросвязи/ИКТ и их программного обеспечения | Продолжение Вопроса 15/11 и Вопроса 17/11 |
| M/11 | Спецификации тестирования протоколов, сетей и услуг для появляющихся технологий, включая оценочное тестированиеи федеративные испытательные стенды | Продолжение Вопроса 16/11 |

# 2 Формулировка Вопросов

ПРОЕКТ ВОПРОСА А/11

Сигнализация и архитектуры протоколов в сетях электросвязи и руководящие указания по реализации с применением появляющихся технологий

(Продолжение Вопроса 1/11)

### А.1 Обоснование

Стремление обеспечивать услуги в сетях и при поддержке сетей обусловило разработку большого количества архитектурных решений многочисленными органами и форумами по стандартизации. Необходима стандартизированная архитектурная модель для управления сигнализацией с учетом сетей на базе LTE (VoLTE/ViLTE), передачи голоса и видеоизображений по стандарту "New Radio" (VoNR/ViNR), NFV и SDN, включая многоконтроллерные сетевые архитектуры SDN, конвергенции связи и вычислений, конвергенции фиксированной, подвижной и спутниковой связи (FMSC), нового поколения услуг связи в реальном времени, нативного искусственного интеллекта (ИИ), технологии распределенного реестра, сетей квантового распределения ключей (QKDN) и связанных с ними технологий, а также других появляющихся технологий электросвязи/ИКТ, которые могут применяться в сетях IMT-2030.

Для плоскости управления требуется стандартная эталонная модель, чтобы определить набор интерфейсов, обеспечивающих функциональную совместимость сетей электросвязи, оборудования различных поставщиков, сетей облачных вычислений, виртуализированных и физических сетей и сетей, находящихся на разных этапах развития, таких как сети IMT-2020 и IMT-2030.

Ввиду того 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 конвергенцию связи и вычислений, конвергенцию фиксированной, подвижной и спутниковой связи (FMSC), нативный 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, заявили о необходимости содействия в понимании стратегий и сценариев развертывания сетей и услуг путем разработки руководящих указаний по реализации протоколов сигнализации для сетей и услуг.

В рамках данного Вопроса будет продолжено ведение предыдущих Технических отчетов и Руководящих указаний по реализации сигнализации и протоколов, разработанные для оказания содействия развивающимся странам. Кроме того, в рамках этого Вопроса будет осуществляться ведение действующих Рекомендаций, которые относятся к сфере ответственности Вопроса, например Рекомендаций МСЭ-Т Q.3030, Q.3040, Q.3050 и Q. 3051.

### 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 конвергенция связи и вычислений, конвергенция фиксированной, подвижной и спутниковой связи (FMSC), нативный ИИ, технология распределенного реестра, QKDN и связанные с ними технологии и т. д., а также технологии, применяемые в сетях IMT‑2030, 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, VoNR/ViNR и IMT-2020 и IMT-2020, включая eMBB, mMTC и uRLLC, а также других новых дополнительных услуг, включенных в сети IMT‑2030?

– Какая требуется работа по подготовке Секторами МСЭ-T и МСЭ-D общих руководящих указаний по различным аспектам, 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 разработки сигнализации и протоколов для появляющихся сетей электросвязи в 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 при помощи 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 сети IMT-2020 и IMT-2030 и т. д.);

− изучение архитектуры сигнализации и управления для моделирования плоскости управления сетей электросвязи с применением появляющихся технологий, таких как конвергенция связи и вычислений, конвергенция фиксированной, подвижной и спутниковой связи (FMSC), нативный ИИ, технология распределенного реестра, QKDN и связанные с ними технологии и т. д., а также технологии, применяемые в сетях IMT-2020;

− 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 с 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://itu.int/ITU-T/workprog/wp\_search.aspx?sg=11](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, в особенности Вопросы, относящиеся к архитектурам и протоколам сигнализации

Исследовательские комиссии

− ИК2, ответственная за аспекты ENUM

− ИК13, ответственная за архитектуру существующих и появляющихся сетей

− ИК15, ответственная за транспортирование

− 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

ПРОЕКТ ВОПРОСА 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, периферийные вычисления с множественным доступом (MEC), DLT и машинное обучение/искусственный интеллект, цифровые двойники, робототехника, сети квантового распределения ключей (QKDN) и связанные с ними технологии, а также другие появляющиеся технологии электросвязи/ИКТ будут способствовать развитию новых протоколов сигнализации для обеспечения взаимодействия и надлежащей связи в сетях IMT-2020 и IMT-2030. 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, иммерсивные вызовы, 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 среде появляющихся технологий электросвязи?

– Какие новые требования к сигнализации и протоколы необходимо разработать для поддержки услуг в сетях электросвязи, включая робототехнику, развивающихся в направлении сетей IMT-2020 и IMT-2030?

– 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, интерактивной 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 будущих услуг в сетях электросвязи, развивающихся в направлении сетей IMT-2020 и IMT-2030;

– 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, интерактивной 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 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

– 3GPP

Направления деятельности ВВУИО

– C2, C5, C11

Цели в области устойчивого развития

– 9

ПРОЕКТ ВОПРОСА 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 IMT-2030, конвергенции наземных и спутниковых сетей, передачи видеоизображения и голоса по сетям на базе LTE (VoLTE/ViLTE), передачи голоса и видеоизображений по стандарту "New Radio" (VoNR/ViNR), межмашинной связи (M2M), интернета вещей (IoT), технологии распределенного реестра, машинного обучения/искусственного интеллекта, сетей квантового распределения ключей (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 возможности использования некоторых появляющихся технологий и прикладных услуг в интересах электросвязи в чрезвычайных ситуациях.

Необходимо также продолжать разработку приложений для электросвязи в чрезвычайных ситуациях, например требований к передаче голоса, изображений и 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, Q.3647, 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 реализации приоритетной связи для пользователей электросвязи в чрезвычайных ситуациях; усовершенствования IEEE в отношении стандартов серии 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 IMT-2030?

− 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 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 IMT-2030;

− 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

– ИК13 МСЭ-T

– ИК16 МСЭ-T

– ИК17 МСЭ-T

– ИК20 МСЭ-T

– ИК5 МСЭ-R

– ИК1 МСЭ-D

Другие органы

– ARIB

– ATIS

– IETF

– IEEE

− ЕТСИ

– TIA

– TTA

– TTC

– 3GPP

Направления деятельности ВВУИО

– C2, C5

Цели в области устойчивого развития

– 9, 11, 13, 16

ПРОЕКТ ВОПРОСА D/11

Протоколы для контроля сетевых ресурсов, управления ими и их оркестровки

(Продолжение Вопроса 4/11)

### D.1 Обоснование

Резолюция 77 (Пересм. Хаммамет, 2016 г.) ВАСЭ направлена на активизацию работы по стандартизации в области организации сетей с программируемыми параметрами (SDN) в Секторе стандартизации электросвязи МСЭ, и в ней поручается исследовательским комиссиям МСЭ-Т продолжать расширять и ускорять работу по стандартизации SDN, в особенности SDN операторского класса, провести исследование состояния развития появляющихся технологий, таких как технология NFV, платформа Container/Docker, для развития технологии SDN, а также продолжать разработку стандартов МСЭ-Т по SDN в целях повышения функциональной совместимости продуктов управления.

В рамках деятельности по данному Вопросу была разработана серия Рекомендаций по контролю, управлению и оркестровке ресурсов сети доставки информации, относящихся к моделям данных, требованиям к сигнализации и протоколам. Ожидается, что стандартизация вышеупомянутого аспекта продолжится на основе сетевых технологий, включая, помимо прочего, сети с программируемыми параметрами (SDN) и другие связанные технологии программизации сетей, виртуализацию сетевых функций (NFV), распределенную оркестровку, цепочки функций услуг, "нарезку" сетей и осведомленные об услугах сети, сети вычислительной мощности, организацию сетей облачных вычислений, виртуализацию сетей, переход к IPv6, организацию ориентированных на большие данные сетей, сеть без потерь, сети IMT-2020 и будущие сети (FN), продолжится и распространится на другие появляющиеся технологии поддержки ИТ, используемые для сети доставки информации, такие как искусственный интеллект/машинное обучение (ИИ/МО), технология распределенного реестра, распределенное облако, периферийные вычисления с множественным доступом (MEC), микросервисная архитектура и конфиденциальные вычисления.

Автоматизация сети, одна из основных тенденций в развитии сетей, способствует гибкости конфигурации и развертывания сети, а также делает всю сеть более предсказуемой и единообразной. Автоматизация сети может быть реализована на основе набора некоторых упомянутых выше сетевых и соответствующих технологий поддержки ИТ, а также на основе стандартизованных языков, инструментов и процессов моделирования.

Поведение трафика, генерируемого все большим количеством новых услуг, таких как услуги, предоставляемые SDN и другими связанными программируемыми сетями, сетями вычислительной мощности и другими новыми технологиями поддержки ИТ, используемыми для сети доставки информации, сильно отличается от поведения трафика, генерируемого традиционными услугами СПП. Соответственно, архитектура управления таким новым трафиком может стать более сложной, а соответствующие требования к сигнализации сети доставки информации тесно связаны с новыми 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.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, Добавление 51 серии Q, Добавление 67 серии Q, Q.3316, Q.3405, Q.3716, Q.3718, Q.3740, Q.3741,Q.3059, Q.3061, Q.4067, Q.3406, Q.4140 и Q.5006.

### D.2 Вопрос

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

– Какие модели данных, требования к сигнализации и протоколы необходимы для контроля, управления и оркестровки сетевых ресурсов, включая новые типы транспортных протоколов и транспортных сетей (такие, как программизация сетей, организация сетей облачных вычислений, интеллектуальные сети, FN, SDN, NFV, распределенная оркестровка, виртуализация сетей, "нарезка" сетей, сети без потерь, MEC, микросервисная архитектура и сети IMT-2020)?

− Какие модели данных, требования к сигнализации и протоколы необходимы для сетей, ориентированных на большие данные 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 облачных и распределенных облачных сетей?

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

– Какие модели данных, требования к сигнализации и протоколы необходимы для формирования цепочек функций услуг?

– Какие модели данных, требования к сигнализации и протоколы необходимы для сети, осведомленной об услугах?

– Какие API, модели данных, требования к сигнализации и протоколы требуются для автоматизации сети?

− Какие новые Рекомендации требуются для поддержки управления переносом информации 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 управления и сигнализации для переноса информации и ресурсов?

− Какие новые усовершенствования функциональной архитектуры и протоколов необходимы для поддержки управления переносом информации 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 переносу информации для поддержки трафика новых приложений на основе архитектур будущих сетей, включая программизацию сетей, SDN, NFV, распределенную оркестровку, виртуализацию сетей, MEC, микросервисную архитектуру, "нарезку" сетей, сети без потерь, облачные и распределенные облачные сети, сети IMT-2020 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 облачных и распределенных облачных сетей;

– 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 сети вычислительных мощностей;

– разработка моделей данных, требований к сигнализации и протоколов для формирования цепочек функций услуг;

– разработка моделей данных, требований к сигнализации и протоколов для сети, осведомленной об услугах;

– разработка API, моделей данных, требований к сигнализации и протоколов для автоматизации сети;

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

− разработка требований к сигнализации и протоколов для управления переносом информации 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 переносом информации 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 переносом информации и ресурсами;

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

− совершенствование существующих Рекомендаций, касающихся управления переносом информации и ресурсами и сигнализации;

− проведение исследований и разработка Рекомендаций в целях определения требований к механизмам управления переносом информации 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

Резолюции

– Резолюция 77 (Пересм. Хаммамет, 2016 г.) ВАСЭ

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, серия Y.3300, серия Y.2501, серия Q.35xx, серия Q.37xx, серия Q.33xx, серия Q.34xx

Вопросы

– Все Вопросы ИК11

Исследовательские комиссии

− ИК2, ответственная за эксплуатационные аспекты

− 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, сети вычислительных мощностей, организацию облачных и распределенных облачных сетей, виртуализацию сетей, "нарезку" сетей, MEC, организацию сетей, ориентированных на большие данные, сети на основе ИИ/МО и сети IMT-2020 и дальнейших поколений

Другие органы

− 3GPP

– ЕТСИ

– IEEE

– IETF

– TIA

– Linux Foundation projects

– OpenInfra Foundation

– Open Networking Foundation (ONF)

Направления деятельности ВВУИО

– C2, C11

Цели в области устойчивого развития

– 9

ПРОЕКТ ВОПРОСА E/11

Требования к сигнализации и протоколы для пограничного шлюза 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, в особенности с развитием сетевой архитектуры в направлении виртуализации, открытости и интеллектуализации, происходит постоянное совершенствование формы устройств и развертывание сервисных функций пограничного шлюза 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 пограничного шлюза 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 несколько пограничных шлюзов сети и дополнительных услуг (VAS) по организации открытых сетей.

С появлением новых технологий также постепенно развивается сетевая архитектура операторов. Требуется, чтобы пограничный шлюз 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 пограничному шлюзу 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 применением 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 применением появляющихся технологий?

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

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

– Какие новые интерфейсы, протоколы и функции пограничного шлюза 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 пограничном шлюзе сети для доставки многих услуг?

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

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

– Какие новые интерфейсы, протоколы и функции необходимо реализовать для пограничного шлюза сети, чтобы поддерживать дифференцированные требования (такие как пропускная способность, задержка, коэффициент потерь пакетов и т. д.) для разных пользователей?

– Какие необходимые новые протоколы и процедуры для пограничного шлюза сети в целях обеспечения возможности масштабируемого и гибкого управления микросервисами и ресурсами?

– Какие новые протоколы и процедуры необходимо определить для дифференцированного спроса на развертывание пограничных шлюзов сети в сетях мегаполисов и кампусов?

### 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 пограничные шлюзы сети с применением появляющихся технологий;

– разработка новых протоколов и процедур для реализации сети вычислительных мощностей между несколькими пограничными шлюзами сети;

− разработка новых требований, протоколов и функций для пограничного шлюза 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 пограничного шлюза 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 пограничного шлюза 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 пограничными шлюзами сети с помощью ИИ;

– разработка новых протоколов и процедур для пограничного шлюза сети, обеспечивающих возможность идентификации приложений и использование сетевых ресурсов в соответствии с подписанным SLA;

– разработка новых протоколов и процедур для пограничного шлюза сети, обеспечивающих возможность масштабируемого и гибкого управления микросервисами и ресурсами посредством гибкого планирования ресурсов;

– разработка новых протоколов и процедур для пограничного шлюза сети с дифференцированными требованиями для развертывания в мегаполисах и кампусных сетях.

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

− Все Вопросы ИК11 МСЭ-Т

Исследовательские комиссии

− ИК13 МСЭ-T и другие ИК, работающие в области СПП, будущих сетей, сетей IMT-2020 и шлюзами широкополосной сети

− ИК20 МСЭ-T

Другие органы

– Форум по широкополосному доступу

– IETF

− ЕТСИ

– ONAP (ПО с открытым исходным кодом)

Направления деятельности ВВУИО

– C2

Цели в области устойчивого развития

– 9

ПРОЕКТ ВОПРОСА F/11

Протоколы, поддерживающие технологии контроля и управления для сетей Международной подвижной электросвязи

(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, микросервисная архитектура, "нарезка" сети, представление возможностей сети, чувствительная ко времени сеть, верификация целостности данных и интеллектуальный сетевой анализ, в целях реализации сети IMT‑2020.

Применение в сетях 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 IMT‑2030. В частности, следует разработать протоколы для поддержки интеллектуального управления в сетях IMT-2020 и IMT-2030, усовершенствованные механизмы, обеспечивающие малую 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 IMT‑2030, разработанных соответствующими ИК МСЭ-T и другими ОРС?

– Какие протоколы и механизмы необходимо определить для ключевых технологий, применяемых при реализации сетей IMT-2020 и IMT-2030, включая интеллектуальное управление для "нарезки" сети, представление возможностей сети, представление возможностей сети, конвергенцию фиксированной и подвижной связи, сетевое управление разнородными сетевыми средами, управление энергоэффективностью, управление сетевыми знаниями, распределенную базовую сеть, распределенную оркестровку, автономную сеть, координацию вычислений и организации сетей и т. д.?

– Как появляющиеся технологии, включая ИИ, большие языковые модели (LLM). большие данные, цифровых двойников, технологию распределенного реестра (DLT), а также сети квантового распределения ключей (QKDN) и связанные с ними технологии, используются в протоколах контроля и управления для сетей IMT-2020 и IMT-2030?

– Какие протоколы и механизмы следует определить для поддержки интегрированного зондирования и связи для сетей IMT-2020 и IMT-2030?

– Какие протоколы и механизмы следует определить для реализации высокопроизводительных и детерминированных SLA с такими характеристиками, как сверхмалая задержка и высокая надежность, для сетей IMT-2020 и IMT-2030?

– Какие протоколы и механизмы следует определить для реализации улучшений и усовершенствований интерфейса на основе услуг для сетей IMT-2020 и IMT-2030 в целях повышения эффективности, гибкости и интеллекта?

– Как использовать и сопровождать программное обеспечение с открытым исходным кодом в сотрудничестве с соответствующими организациями, деятельность которых связанна с ключевых технологиями сетей IMT-2020 и IMT-2030, 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 IMT-2030 с расширенными функциями, поддерживающими сверхбольшую сеть, гибкое установление соединений и гибкую топологию, конвергенцию фиксированной/подвижной и спутниковой связи, оптимизацию плоскости пользователя, эффективность использования зеленой энергии и т. д.;

– разработка Рекомендаций по протоколам, включая механизмы, для поддержки сетей IMT-2020 и IMT-2030 с использованием таких технологий, как "нарезка" сети, виртуализация ресурсов, оркестровка, распределенная базовая сеть, распределенная оркестровка, автономная сеть, координация вычислений и организации сетей, а также сопутствующие технологии и т. д.;

– разработка Рекомендаций по протоколам, включая механизмы, для поддержки сетей IMT-2020 и IMT-2030 с использованием таких технологий, как большие данные, QKDN, цифровой двойник, DLT, ИИ, включая LLM и граф знаний и т. д.;

– разработка Рекомендаций по протоколам, включая механизмы, для поддержки интегрированного зондирования и связи для сетей IMT-2020 и IMT-2030;

– разработка Рекомендаций по протоколам, включая механизмы, для других ключевых технологий сетей IMT-2020 и IMT-2030, включая идентификацию, аутентификацию устройств, представление возможностей сети и т. д.;

– разработка Рекомендаций по протоколам, включая механизмы, для общей системы управления сетями IMT-2020 и IMT-2030;

– разработка Рекомендаций по протоколам, включая механизмы, для сетей IMT-2020 и IMT-2030 в целях реализации высокопроизводительных и детерминированных SLA с такими характеристиками, как сверхмалая задержка и высокая надежность, для сетей IMT-2020 и IMT-2030;

– разработка Рекомендаций по протоколам для сетей IMT-2020 и IMT-2030 в целях реализации улучшений и усовершенствований интерфейса на основе услуг для повышения эффективности, гибкости и интеллекта;

– разработка, в сотрудничестве с соответствующими органами, Добавлений, Технических отчетов, Руководящих указаний по передовому опыту и реализации протоколов и механизмов для сетей IMT-2020 и IMT-2030, 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

– Все Вопросы ИК11

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 по IMT-2020

Другие органы

– МСЭ-R

– ЕТСИ

– IETF

– IEEE

– 3GPP

Направления деятельности ВВУИО

– C2, C5

Цели в области устойчивого развития

– 9, 17

ПРОЕКТ ВОПРОСА G/11

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

(Продолжение Вопроса 7/11)

### G.1 Обоснование

ИК11 МСЭ-T проводила исследование требований к сигнализации и протоколов для будущих сетей. Актуальной темой были периферийные вычисления, необходимые для искусственного интеллекта (ИИ), 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, ИИ, 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, системы видеонаблюдения и т.д.) и среду облачных вычислений (периферийное облако, общедоступное облако 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 реализации таких вычислений. 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 услуги, управление подсоединением и распределение ресурсов для периферийных вычислений.

Кроме того, IMT-2020 может повысить скорость трафика пакетов данных в десять раз по сравнению с IMT-advanced, тогда как периферийные вычисления сокращают задержку транзакций благодаря размещению вычислительных мощностей в сети IMT-2020 ближе к конечным пользователям подвижной связи. В этом аспекте возможности облачных вычислений также важны для обеспечения транзакций данных со сверхмалой задержкой для услуг, требующих малой задержки и высокой пропускной способности (например, 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, автономное вождение, роботы, сельское хозяйство, энергетика, образование, городская воздушная мобильность 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), включая многоконтроллерные сетевые архитектуры 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 сигнализации 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 сетей 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 сигнализации для поддержки пересмотра требований к протоколу присоединения к сетям и периферийных вычислений;

− разработка требований к сигнализации и протоколов сигнализации для поддержки процедур подсоединения к сетям и периферийных вычислений для различных появляющихся услуг (такие как AR/VR, потоковая передача, игры, ИИ, большие данные, автономное вождение, роботы, сельское хозяйство, энергетика, образование, городская воздушная мобильность, цифровые близнецы и т. д.) с использованием нескольких устройств, нескольких соединений и нескольких интерфейсов для будущих сетей (например, SDN, NFV) и сетей IMT-2020;

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

– разработка требований к сигнализации и протоколов сигнализации 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 малой задержкой IMT-2020;

– 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 ИК11 МСЭ-Т

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

ПРОЕКТ ВОПРОСА Н/11

Протоколы, поддерживающие организацию сетей распределенного контента и технологии сети, ориентированной на информацию (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 услуги, такие как распределенное обучение, распределенный реестр, цифровой двойник, и диалоговые мультимедийные услуги, такие как IPTV, цифровой информационный экран, видео по запросу (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 ХR, UHD (4K, 8K) и метавселенная. 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 рабочие характеристики и возможность масштабирования связи. ИК11 МСЭ-Т разрабатывает Рекомендации по архитектуре и протоколам сигнализации для управляемого обмена данными 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 эффективные и гибкие возможности распределения информации для услуг, связанных с IoT, и услуг на основе технологии распределенного реестра (DLT). 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 сетей, ориентированных на информацию (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 ICN при развертывании наложенных сетей, нижележащих сетей и виртуализированной IP-инфраструктуры, составят очень важные новые вопросы для обеспечения соответствующих требований и возможностей сетей IMT‑2020.

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 обмена данными).

### 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 и будущих сетей, 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?

– Какие протоколы и механизмы необходимо разработать для поддержки распределенных услуг на базе управляемого и гибридного однорангового обмена данными?

– 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;

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

– разработка Рекомендаций по протоколам и механизмам для поддержки управляемого и гибридного однорангового обмена данными;

− разработка Рекомендаций по протоколам для поддержки сквозных многосторонних и распределенных услуг, включая потоковую передачу мультимедиа, потоковую передачу данных, метавселенную, распределенное обучение, распределенный реестр, цифровой двойник.

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 МСЭ‑T

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

ПРОЕКТ ВОПРОСА 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 перспективы приложений, услуг и технологий IoT, которые могут быть обеспечены радиочастотной идентификацией (RFID), повсеместно распространенной сенсорной сетью (ПРСС), машинно-ориентированной связью (MOC), цифровыми двойниками, межмашинной (M2M) связью, связью "умных" устройств (SDC), облачными услугами IoT (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 соединений, включая неназемные сети, 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.

Приложение IoT состоит из услуг, не подконтрольных приложению, и единственный способ, с помощью которого могут выполняться стратегии автоматизации тестирования, заключается в том, чтобы включить ИИ и машинное обучение. За счет использования ИИ и ML для тестирования IoT и его приложений возможно сократить время и затраты путем автоматизации емких и подверженных ошибкам задач, таких как создание тестовых примеров, генерация тестовых данных, выполнение тестов и проверка результатов.

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 или интеллектуальная транспортная система;

– летающие сети на базе беспилотных летательных аппаратов;

– "умная" зарядная инфраструктура для электрических транспортных средств.

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 новые Рекомендации необходимо разработать, для обеспечения механизмов тестирования устройств IoT, используемых в неназемных сетях (NTN)?

– Какие наборы тестов необходимо разработать для тестирования IoT и его приложений с использованием ИИ и МО?

– Какие требования и методики тестирования необходимо разработать для тестирования IoT и его приложений с использованием цифровых двойников?

– 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 устройств IoT, используемых в неназемных сетях (NTN);

– разработка наборов тестов для тестирования IoT и его приложений с использованием ИИ и МО;

– разработка методики тестирования и требований для тестирования IoT и его приложений с использованием цифровых двойников;

– 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

– Все Вопросы ИК11 МСЭ-Т

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

– 3GPP

Направления деятельности ВВУИО

– C5

Цели в области устойчивого развития

– 9

ПРОЕКТ ВОПРОСА J/11

Мониторинг и измерение 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 некоторые появляющиеся сети, включая будущие сети (FN), интернет вещей (IoT), сети IMT-2020 и IMT-2030 и т. д. В целях сокращения инвестиций и эксплуатационных затрат в появляющихся сетях развернуты сети с программируемыми параметрами (SDN), а также внедряется виртуализация сетевых функций (NFV), микросервисная архитектура, с тем чтобы обеспечить разделение управления и услуг, управления и переноса информации, аппаратного и программного обеспечения. Мониторинг сред SDN/NFV помогает операторам и администраторам обеспечить бесперебойную работу виртуализированных сетевых функций и корректное применение сетевых политик.

Облачные и периферийные вычисления также становятся цифровой инфраструктурой. В этой новой среде критическое значение для операторов и конечных пользователей имеет наличие возможностей мониторинга для гарантии того, что используемая ими инфраструктура может поддерживать приложения и услуги. Мониторинг облачных и периферийных вычислений помогает гарантировать, что данные обрабатываются эффективно, а периферийные устройства работают должным образом.

Все более широкое применение технологии ИИ в сетях обеспечивает для операторов и интернет‑предприятий возможности интеллектуального принятия решений и интеллектуального прогнозирования. Выбор подлежащих мониторингу параметров в модели интеллектуального принятия решений или интеллектуального прогнозирования в значительной степени влияет на эффективность сети и в итоге – на взаимодействие с пользователями. Мониторинг систем ИИ помогает гарантировать, что они делают точные прогнозы и принимают соответствующие меры.

Стандартизация параметров системы мониторинга для появляющихся сетей, включая облачные вычисления, предоставит операторам, администраторам и конечным пользователям информацию мониторинга, 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 мониторинга рабочих характеристик сети?

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

– Каким является минимальный набор параметров, который необходимо использовать для мониторинга NFV и SDN, включая микроуслуги?

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

− Параметры какого вида необходимо использовать для применения технологии ИИ в появляющихся сетях, приложениях и услугах?

− Каким является минимальный набор параметров, который необходимо использовать для мониторинга 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, включая микроуслуги;

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

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

− изучение видов параметров, которые необходимо использовать в интеллектуальных сетях, приложениях и услугах.

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

– Все Вопросы ИК11 МСЭ-Т

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

– C1, C2, C5

Цели в области устойчивого развития

– 1, 7, 9, 17

ПРОЕКТ ВОПРОСА K/11

Тестирование облачных/периферийных 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. Периферийные вычисления – это вычислительная технология для развертывания возможностей обработки на границе сети, где соединяются оконечные устройства, и для обработки данных, получаемых от оконечных устройств и подаваемых на оконечные устройства. Организация сетей с программируемыми параметрами (SDN) – это набор технологий, позволяющих напрямую выполнять программирование, оркестровку, контроль сетевых ресурсов и управление ими, что облегчает проектирование, доставку и эксплуатацию сетевых услуг динамичным и масштабируемым образом. Виртуализация сетевых функций (NFV) – это принцип отделения сетевых функций от аппаратного обеспечения, на котором они работают, с помощью метода виртуальной аппаратной абстракции.

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

В контексте облачных вычислений/периферийных вычислений, архитектуры микросервисов, SDN/NFV проверка соответствия – это тестирование для проверки того, что реализация облачных вычислений/периферийных вычислений/SDN/NFV соответствует разработанному стандарту, например стандарту функциональных требований или спецификации протокола. Проверка на функциональную совместимость – это тестирование для оценки способности объектов, участвующих в облачных вычислениях/периферийных вычислениях/SDN/NFV, взаимодействовать друг с другом ожидаемым образом. Оценочное тестирование используется для измерения реализации облачных вычислений/периферийных вычислений/SDN/NFV в части рабочих характеристик.

Кроме того, с использованием технологий облачных/периферийных вычислений, SDN и NFV, таких как SD-WAN, сеть вычислительных мощностей (CPN), реализуется все больше и больше услуг. Необходимо рассмотреть возможность тестирования услуг на основе облачных/периферийных вычислений, SDN и NFV.

Необходимо сотрудничество с 13-й Исследовательской комиссии МСЭ-Т (ведущей ИК по будущим вычислениям и будущим сетям с технологиями, связанными с SDN/NFV) в области тестирования облачных/периферийных вычислений, SDN и NFV. Проведение тестирования, связанного с облачными/периферийными вычислениями, SDN и NFV, начнется после того, как ИК13 определит терминологию, требования и архитектуру.

### K.2 Вопрос

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

– Какова структура тестирования на соответствие, функциональную совместимость и оценочного тестирования облачных/периферийных вычислений, SDN, NFV и архитектуры микроуслуг?

– Какие наборы тестов необходимы для тестирования облачных/периферийных вычислений, SDN и NFV, а также архитектуры микроусдуг, включая аспект соответствия, функциональной совместимости и оценочного тестирования?

– Как создать автоматизированную систему тестирования облачных/периферийных вычислений, SDN и NFV, а также архитектуры микроусдуг для повышения эффективности тестирования?

– Какие наборы тестов необходимы для тестирования услуг, реализуемых средствами облачных/периферийных вычислений, SDN и NFV, а также архитектуры микроусдуг, например тестирование SD-WAN и CPN?

– 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 структуры тестирования на соответствие, функциональную совместимость и оценочного тестирования облачных/периферийных вычислений, SDN, NFV и архитектуры микроуслуг;

– разработка наборов тестов для тестирования на соответствие, функциональную совместимость и оценочного тестирования облачных/периферийных вычислений, SDN, NFV и архитектуры микроуслуг;

– разработка методики и структуры автоматизированного тестирования облачных/периферийных вычислений, SDN, NFV и архитектуры микроуслуг;

– разработка наборов тестов для тестирования услуг, реализуемых средствами средствами облачных/периферийных вычислений, SDN и NFV, а также архитектуры микроусдуг;

– 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 МСЭ-Т

Исследовательские комиссии

– ИК2, ответственная за эксплуатационные аспекты

– ИК12, ответственная за QoS/QoE

– ИК13, ответственная за будущие сети 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

ПРОЕКТ ВОПРОСА L/11

Борьба с использованием контрафактных и похищенных устройств электросвязи/ИКТ и их программного обеспечения

(Продолжение Вопроса 15/11 и Вопроса 17/11)

### L.1 Обоснование

В Резолюции 188 (Пересм. Бухарест, 2022 г.) Полномочной конференции МСЭ признаются отрицательные последствия, создаваемые контрафактными устройствами электросвязи/ИКТ для органов государственной власти, производителей, поставщиков и потребителей, а также, 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 контрафактными устройствами электросвязи/ИКТ. Определять подлинные продукты возможно с помощью любых уникальных и стойких идентификаторов. Кроме того, особое внимание следует уделять потенциальному росту числа контрафактных устройств IoT и его возможным последствиям.

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. Бухарест, 2022 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 принято решение изучить этот вопрос и стимулировать разработку способов и средств продолжения борьбы с хищением мобильных устройств и предотвращения этого явления, и предлагается Государствам-Членам предпринимать шаги, требуемые для предотвращения, обнаружения и контроля подделки и копирования идентификаторов мобильных устройств ИКТ.

В Резолюции 97 (Пересм. Женева, 2022 г.) Всемирной ассамблеи по стандартизации электросвязи признается, что хищение принадлежащих пользователям мобильных устройств может привести к преступному использованию услуг и приложений электросвязи/ИКТ, что повлечет за собой экономический ущерб для законного владельца и пользователя, и указывается на необходимость определить существующие и будущие технологические меры с применением программных и аппаратных средств для смягчения последствий использования похищенных мобильных устройств.

Работа в рамках этого Вопроса в основном сосредоточена на разработке Рекомендаций и Технических отчетов по борьбе с контрафактными и поддельными устройствами и программным обеспечением 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 сопровождается увеличением количества 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 списков заблокированных 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.

Кроме того, как правило, пользователь электросвязи/ИКТ не осведомлен об уязвимостях, которые содержатся в контрафактных устройствах или могут присутствовать в контрафактном или поддельном программном обеспечении ИКТ. Несколько примеров:

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 в сеть пользователя, что позволяет похищать данные и чревато потерей доходов;

iii) контрафактное/поддельное программное обеспечение в устройствах ИКТ, которое позволяет лицам, не являющимся абонентами, получить несанкционированный доступ к данным поставщика контента.

Поэтому крайне важно повышать степень осведомленности всех заинтересованных сторон по этой теме.

Данный Вопрос направлен на изучение соответствующих возможностей борьбы с использованием похищенных и контрафактных или поддельных устройств и программного обеспечения электросвязи/ИКТ, в частности, их связи с управлением определением идентичности в цепочке поставки продуктов, отслеживаемостью, безопасностью, конфиденциальностью, доверием людей и сетей. Для сбора полной информации и понимания этого вопроса, в том числе для организации в сотрудничестве со всеми заинтересованными сторонами семинаров/практикумов, 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 серий 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 и руководящие указания необходимы для повышения уровня осведомленности о проблеме контрафакции устройств ИКТ, подделки программного обеспечения ИКТ и незаконного присвоения данных ИКТ и об опасностях, которые они представляют?

– Достаточны ли существующие механизмы уникальных идентификаторов устройств для борьбы с контрафактными, поддельными и похищенными устройствами электросвязи/ИКТ?

– Возможно ли использовать системы проверки на соответствие и функциональную совместимость и системы их оценки для борьбы с контрафактными и поддельными устройствами электросвязи/ИКТ и их программным обеспечением?

– Какие технологии и решения возможно использовать в качестве инструмента борьбы с контрафактными, поддельными и похищенными устройствами электросвязи/ИКТ и их программным обеспечением?

– Какие структуры уникальных идентификаторов устройств подходят для борьбы с контрафактными и похищенными устройствами электросвязи/ИКТ с измененными идентификационными данными?

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

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

– Какого вида Рекомендации, Добавления, Технические отчеты и Руководящие указания следует разработать для борьбы с контрафакцией в сфере 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 предотвращения незаконного присвоения данных ИКТ, в частности данных пользователей, содержащихся в устройствах ИКТ, и контента, предоставляемого поставщиками услуг ИКТ?

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

– Какого вида Рекомендации, Добавления, Технические отчеты и Руководящие указания следует разработать в помощь Членам МСЭ, в сотрудничестве с Сектором МСЭ-D, в борьбе с контрафактным или поддельным программным обеспечением электросвязи/ИКТ, хищением, незаконным присвоением и проблемами, которые они вызывают?

– Какие Рекомендации, Добавления, Технические отчеты и Руководящие указания МСЭ требуются для безопасного управления цепочкой поставок (от производства до ввоза, распределения и сбыта) в целях повышения отслеживаемости, безопасности, конфиденциальности и доверия со стороны людей, продуктов и сетей?

– 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 в помощь Членам МСЭ, в сотрудничестве с Сектором МСЭ-D, в борьбе с контрафактными и поддельными устройствами электросвязи/ИКТ и их программным обеспечением и последующим незаконным присвоением данных;

– разработка Рекомендаций, Добавлений, Технических отчетов и Руководящих указаний по показателям работы и пробелам в существующих механизмах уникального идентификатора устройств для борьбы с контрафактными, поддельными и похищенными устройствами электросвязи/ИКТ на основе сценариев использования членами МСЭ;

− разработка Рекомендаций, Добавлений, Технических отчетов и Руководящих указаний в помощь Членам МСЭ, в сотрудничестве с Сектором МСЭ-D, в борьбе с контрафактными устройствами IoT;

– разработка Рекомендаций, Добавлений, Технических отчетов и Руководящих указаний для решения проблемы похищенных устройств электросвязи/ИКТ и в помощь Членам МСЭ, в сотрудничестве с Сектором МСЭ-D, при внедрении решений для смягчения последствий использования похищенных устройств;

– разработка Рекомендаций, Добавлений, Технических отчетов и Руководящих указаний для определения новых категорий устройств электросвязи/ИКТ, для которых может быть обеспечен выигрыш в результате борьбы с контрафакцией, а также для определения типов идентификаторов устройств, которые следует рассмотреть для каждой категории;

– изучение соответствующих решений, включая структуры уникальных идентификаторов устройств, для борьбы с контрафактными и похищенными устройствами электросвязи/ИКТ с поддельными или дублированными уникальными идентификаторами;

– изучение соответствующих технологий, которые возможно использовать в качестве инструмента борьбы с контрафактными, поддельными и похищенными устройствами электросвязи/ИКТ;

– исследование ущерба, который наносит заинтересованным сторонам использование контрафактных устройств электросвязи/ИКТ или устройств с поддельным или контрафактным программным обеспечением и последующее незаконное присвоение данных;

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

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

– изучение возможных решений по проверке на соответствие и функциональную совместимость (C&I) для борьбы с контрафакцией и подделкой устройств электросвязи/ИКТ и их программного обеспечения, а также последующего незаконного присвоения данных, 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

– Резолюции 188, 189 (Пересм. Бухарест, 2022 г.) Полномочной конференции

– Резолюция 79 (Пересм. Кигали, 2022 г.) ВКРЭ;

– Резолюции 76, 97 (Пересм. Женева, 2022 г.) ВАСЭ и Резолюция 96 (Пересм. Хаммамет, 2016 г.) ВАСЭ.

Рекомендации

− МСЭ-T X.1127, МСЭ-T X.1255, МСЭ-T X.660, МСЭ-T Q.5050, МСЭ-T Q.5051, МСЭ-T Q.5052, МСЭ-T Q.5053

Вопросы

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

Исследовательские комиссии

– ИК2 МСЭ-T

− ИК3 МСЭ-T

− ИК5 МСЭ-T

− ИК12 МСЭ-T

− ИК13 МСЭ-T

− ИК16 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

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

ПРОЕКТ ВОПРОСА M/11

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

(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* указано, что 11-я Исследовательская комиссия МСЭ-T продолжает координировать деятельность Сектора, касающуюся программы МСЭ в области соответствия и функциональной совместимости (C&I), во всех исследовательских комиссиях и продолжает осуществлять деятельность в рамках программы C&I, включая пилотные проекты по проверке на соответствие/функциональную совместимость.

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, IMT-2030, IoT) могут вызвать 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, VoLTE, ViLTE, VoNR, ViNR, IMT‑2020, IMT-2030), которые, в числе прочих, будут использоваться для услуг роуминга/кочевой связи. Проверка на соответствие и функциональную совместимость интерфейсов сеть-сеть (NNI) по Рекомендациям МСЭ-Т может помочь операторам удостовериться в том, что их сетевые решения готовы для присоединения. Такой подход к присоединению возможно использовать также для будущих сетей на основе пакетов, например сетей IMT-2020, IMT-2030 и дальнейших поколений.

Кроме того, новые ИКТ, сети и отраслевые приложения становятся все более сложными для тестирования с использованием отдельных испытательных стендов. Объединенные в федерацию испытательные стенды обеспечивают устойчивое создание благоприятной среды, способствующей быстрому внедрению инноваций и тестированию сложных технологий и сценариев использования, а также ускорению выхода на рынок продуктов и услуг.

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 наборы 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 типы наборов тестов необходимы для тестирования присоединения сетей на базе IP (таких, как сети IMT-2020, IMT-2030 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?

− Каким образом возможно дистанционно тестировать параметры/технологии/услуги?

– Какие API необходимо разработать для реализации федеративных испытательных стендов?

– Какие пользовательские требования к испытательному стенду как услуге (TaaS) необходимо разработать?

– Как необходимо обновить эталонную модель федеративных испытательных стендов с учетом потребностей рынка?

– Какие руководящие указания необходимо разработать для реализации федеративных испытательных стендов?

– Какова методика тестирования мобильных устройств IMT-2020 и IMT-2030?

– Какова методика тестирования услуг, для которых 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 наборы 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 наборов тестов, которые следует использовать для тестирования присоединения сетей на базе IP (таких, как сети IMT-2020, IMT-2030 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;

– определение параметров/технологий/услуг, которые возможно тестировать дистанционно;

– разработка требований к API, которые следует использовать для федеративных испытательных стендов;

– разработка пользовательских требований к TaaS;

– обновление эталонной модели федеративных испытательных стендов;

– разработка руководящих указаний для реализации федеративных испытательных стендов;

– разработка методики (руководства), которая распространит имеющийся опыт и подходы к тестированию на сети IMT-2020 и IMT-2030;

– 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

− ИК3 МСЭ‑T, ответственная за вопросы политики

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

– 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

– Вопрос 4/2 ИК2 МСЭ-D

Другие органы

– ЕТСИ (в особенности TC INT ЕТСИ)

– IETF

– IEEE

Направления деятельности ВВУИО

– C5, C6

Цели в области устойчивого развития

– 9

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