|  |  |
| --- | --- |
| **Всемирная ассамблея по стандартизации электросвязи (ВАСЭ-20)Женева, 1–9 марта 2022 года** | A picture containing text, clipart  Description automatically generated |
|  |
|  |  |
| **ПЛЕНАРНОЕ ЗАСЕДАНИЕ** | **Пересмотр 1 Документа 22-R** |
|  | **Декабрь 2021 года** |
|  | **Оригинал: английский** |
|  |
| 20-я Исследовательская комиссия МСЭ-Т |
| интернет вещей и "умные" города и сообщества (SC&C) |
| ОТЧЕТ ИК20 МСЭ-Т ВСЕМИРНОЙ АССАМБЛЕЕ ПО СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ (васэ-20): ЧАСТЬ II – ВОПРОСЫ, ПРЕДЛАГАЕМЫЕ ДЛЯ ИССЛЕДОВАНИЯ В ходе СЛЕДУЮЩЕГО ИССЛЕДОВАТЕЛЬСКОГО ПЕРИОДА (2022–2024 гг.) |
|  |

|  |  |
| --- | --- |
| **Резюме**: | В настоящем вкладе содержится текст Вопросов 20‑й Исследовательской комиссии МСЭ-Т, предлагаемых для утверждения Ассамблеей на следующий исследовательский период. В Пересмотре 1 исправлена информация, касающаяся истории Вопросов (таблица на странице 2 и строки после заголовка каждого Вопроса). |
| **Для контактов**: | г-н Нассер Салех Аль-Марзуки (Mr Nasser Saleh Al Marzouqi)Председатель ИК20 МСЭ-Т ОАЭ | Тел.: +971 2 777 2468Факс: +971 2 777 2122Эл. почта: nasser.almarzouqi@tdra.gov.ae |

**Примечание БСЭ**:

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

Часть I: **Документ 21** – Общая информация

Часть II: **Документ 22** – Вопросы, предлагаемые для исследования в ходе исследовательского периода 2022−2024 годов

# 1 Список: семь Вопросов, предлагаемых 20-й Исследовательской комиссией

| Номер Вопроса | Название Вопроса | Статус |
| --- | --- | --- |
| A/20 | Функциональная совместимость и обеспечение взаимодействия приложений и услуг IoT и SC&C | Продолжение Вопроса 1/20  |
| B/20 | Требования, возможности и архитектурные структуры в различных вертикальных отраслях, расширенные за счет появляющихся цифровых технологий | Продолжение Вопроса 2/20  |
| C/20 | Архитектуры, протоколы и QoS/QoE IoT и SC&C | Продолжение Вопроса 3/20 |
| D/20 | Анализ и обработка данных, обмен и управление данными в IoT и SC&C, включая аспекты больших данных | Продолжение Вопроса 4/20 |
| E/20 | Исследование появляющихся цифровых технологий, терминологии и определений | Продолжение Вопроса 5/20 |
| F/20 | Безопасность, конфиденциальность, доверие и идентификация для IoT и SC&C | Продолжение Вопроса 6/20  |
| G/20 | Анализ и оценка "умных" устойчивых городов и сообществ | Продолжение Вопроса 7/20 |

# 2 Формулировка Вопросов

В оставшейся части настоящего документа приводится предлагаемый текст Вопросов.

ВОПРОС А/20

Функциональная совместимость и обеспечение взаимодействия
приложений и услуг IoT и SC&C

(Продолжение Вопроса 1/20)

### A.1 Обоснование

Численность населения городских районов мира стремительно растет, и ожидается, что к 2050 году в городских районах будет проживать 68% населения мира. Столь стремительная урбанизация сопряжена с рисками социальной нестабильности, нарушений работы критической инфраструктуры, кризисов в области водоснабжения и распространения инфекционных заболеваний.

Для решения проблем, возникающих в связи с высокими темпами урбанизации, необходимо повысить эффективность деятельности городов и сообществ (в том числе деревень и малых городов) и использования ими ресурсов.

Повышение эффективности может быть достигнуто путем обеспечения взаимодействия отдельных систем в рамках городов и сообществ, таких как водоснабжение, электроснабжение, утилизация отходов и транспорт, а также путем обмена данными между различными организационными подразделениями городов.

В связи с тем, что многие граждане часто переезжают из города в город, большое значение имеет также взаимодействие между городами.

### A.2 Вопросы

В рамках данного Вопроса рассматриваются сценарии использования, требования, архитектуры, а также наборы и формат данных для поддержки взаимодействия и обеспечения функциональной совместимости приложений и услуг IoT и SC&C не только в рамках отдельных городов и сообществ, но и между ними.

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

– Каковы сценарии использования при взаимодействии приложений и услуг IoT и SC&C?

– Каковы требования и архитектуры для поддержки взаимодействия и обеспечения функциональной совместимости приложений и услуг IoT и SC&C?

– Как обеспечить функциональную совместимость данных и семантическую функциональную совместимость?

### A.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– Разработка соответствующих Рекомендаций, Добавлений, Отчетов, руководящих указаний и т. д., касающихся:

• сценариев использования при взаимодействии приложений и услуг IoT и SC&C в различных вертикальных отраслях;

• требований к обеспечению взаимодействия и функциональной совместимости и их архитектур;

• промежуточного программного обеспечения и платформ для обеспечения взаимодействия и функциональной совместимости;

• наборов и форматов данных для обеспечения функциональной совместимости данных и семантической функциональной совместимости между различными вертикальными отраслями;

• реализации, развертывания, эксплуатации и технического обслуживания в отношении вышеперечисленных задач.

– Обеспечение необходимого сотрудничества для совместной деятельности в этой области в рамках МСЭ, а также между МСЭ-Т и другими соответствующими ОРС, консорциумами и форумами.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК20 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=1/20>.

### A.4 Относящиеся к Вопросу

Направления деятельности ВВУИО

– C2, C3, C5, C6, C7, C8, C10

Цели в области устойчивого развития

– 11

Рекомендации

– Серия Y.4000, в том числе Y.4100/Y.2066, Y.4111/Y.2076, Y.4113, Y.4114, Y.4200, Y.4201, Y.4401/Y.2068, Y.4461, Y.4552/Y.2078

Вопросы

– Все Вопросы ИК20 МСЭ-Т

Исследовательские комиссии

− Соответствующие исследовательские комиссии МСЭ-T (например, с учетом выполнения ими функции ведущей исследовательской комиссии), МСЭ-D и МСЭ-R

– Работа над данным Вопросом предполагает координацию с ИК13 МСЭ-Т по соответствующим аспектам больших данных.

Другие органы

– 3GPP

– ЕТСИ

– SyC МЭК по "умным" городам

– IETF

– ПК41 ОТК1 ИСО/МЭК, РГ11 ОТК1 ИСО/МЭК

– ТК268 ИСО

– Объединенная целевая группа по "умным" городам МЭК/ИСО/МСЭ

– oneM2M

– W3C

ВОПРОС B /20

Требования, возможности и архитектурные структуры в различных вертикальных отраслях, расширенные за счет появляющихся
цифровых технологий

(Продолжение Вопроса 2/20)

### B.1 Обоснование

В связи с постоянно растущим количеством услуг и приложений интернета вещей (IoT) необходимо провести исследование требований, возможностей и архитектурных основ IoT и "умных" городов и сообществ (SC&C). Появляющиеся услуги и приложения IoT предъявляют все больше требований к сетям и к предоставлению новых услуг, в результате чего возникает необходимость во все более высоком уровне интеллектуализации сетей и обеспечении новых возможностей.

Одной из основных задач является максимальное использование общих возможностей и архитектурных структур, с тем чтобы обеспечить поддержку широкого спектра услуг и приложений IoT и SC&C в различных вертикальных отраслях экономически эффективным способом, с участием многих производителей и с возможностью легкого развертывания на основе конвергентных инфраструктур.

В IoT наблюдается растущая интеграция и конвергенция информационно-коммуникационных технологий (ИКТ) и появляющихся цифровых технологий, включая, помимо прочего, периферийные вычисления, искусственный интеллект/машинное обучение (ИИ/МО), блокчейн, виртуальные копии, обработку и анализ данных, технологии оркестровки и автоматизации, появляющиеся сетевые технологии и передовые технологии измерения и срабатывания. Эти технологии предоставляют большой набор расширенных возможностей для поддержки услуг и приложений IoT и SC&C, которые должны быть интегрированы с точки зрения архитектурных структур, исходя как из общих (независимых от вертикальной отрасли) требований, так и требований конкретных вертикальных отраслей.

Необходимо также обеспечить эффективную увязку между стандартами IoT и SC&C и практическими аспектами внедрения, развертывания, эксплуатации и технического обслуживания, с тем чтобы оценить возможности и преимущества использования этих стандартов в конкретных сценариях применения.

### B.2 Вопросы

В рамках этого Вопроса рассматриваются общие и конкретные требования, возможности и архитектурные структуры в различных вертикальных отраслях, расширенные за счет появляющихся технологий.

На основе сценариев использования и связанных с ними экосистемных аспектов будут определены как общие (независимые от вертикальной отрасли), так и зависимые от конкретной вертикальной отрасли требования, возможности и архитектурные структуры для поддержки услуг и приложений IoT и SC&C, расширенные за счет появляющихся технологий.

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

– Каковы сценарии использования приложений и услуг IoT и SC&C в различных вертикальных отраслях?

– Каковы требования, возможности и архитектурные структуры, необходимые для поддержки новых услуг и приложений IoT и SC&C в различных вертикальных отраслях?

– Сотрудничество с какими организациями по разработке стандартов (ОРС) будет необходимым для максимального увеличения синергии и согласования существующих стандартов?

### B.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– Разработка соответствующих Рекомендаций, Отчетов, дорожных карт, руководящих указаний и т. д. для поддержки новых услуг и приложений IoT и SC&C, охватывающих:

• сценарии использования услуг и приложений IoT и SC&C в различных вертикальных отраслях;

• аспекты экосистемы с учетом бизнес-моделей и сценариев использования;

• общие и конкретные требования, возможности и архитектурные структуры в различных вертикальных отраслях, расширенные за счет появляющихся технологий;

• связанные с IoT и SC&C вопросы реализации, развертывания, эксплуатации и технического обслуживания, а также проверки концепций в отношении вышеперечисленных задач.

− Обеспечение необходимого сотрудничества для совместной деятельности в этой области в рамках МСЭ, а также между МСЭ-Т и другими соответствующими ОРС, консорциумами и форумами.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК20 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=2/20>.

### B.4 Относящиеся к Вопросу

Направления деятельности ВВУИО

– C2, C3, C5, C6, C7, C8, C10

Цели в области устойчивого развития

– 9, 10 и 11

Рекомендации

– Серия Y.4000, в том числе Y.4000/Y.2060, Y.4003, Y.4100/Y.2066, Y.4101/Y.2067, Y.4102/Y.2074, Y.4103/F.748.0, Y.4105/Y.2221, Y.4108/Y.2213, Y.4109/Y.2061, Y.4110/Y.2065, Y.4111/Y.2076, Y.4112/Y.2077, Y.4113, Y.4116, Y.4117, Y.4118, Y.4119, Y.4120, Y.4121, Y.4201, Y.4203, Y.4204, Y.4207, Y.4208, Y.4250/Y.2222, Y.4401/Y.2068, Y.4408/Y.2075, Y.4457, Y.4464, Y.4552/Y.2078, Y.4702, Y.Suppl.53, Y.Suppl.56 к Серии Y

Вопросы

– Все Вопросы ИК20 МСЭ-T

Исследовательские комиссии

− Соответствующие исследовательские комиссии МСЭ-T (например, с учетом выполнения ими функции ведущей исследовательской комиссии), МСЭ-D и МСЭ-R

Другие органы

– IETF

– Открытый альянс подвижной связи (OMA)

– Открытый геопространственный консорциум (OGC)

– IEEE

– ATIS

– ТК Smart M2M ЕТСИ

– TC10 CCSA

– oneM2M

– ПК41 ОТК1 ИСО/МЭК, РГ11 ОТК1 ИСО/МЭК

– Объединенная целевая группа по "умным" городам МЭК/ИСО/МСЭ

– Ассоциация GSM

– 3GPP/3GPP2

– W3C

– Организация по развитию стандартов структурированной информации (OASIS)

– Группа управления объектами (OMG)

− Промышленный консорциум интернета (IIC)

– Альянс промышленного интернета (AII)

− Альянс для инноваций в IoT (AIOTI)

– Фонд "Открытые соединения" (OCF)

– Альянсы 5G (например, 5G AA, 5G ACIA и др.)

ВОПРОС C/20

Архитектуры, протоколы и QoS/QoE IoT и SC&C

(Продолжение Вопроса 3/20)

### C.1 Обоснование

Поскольку интернет вещей (IoT) завоевывает позиции как один из основных механизмов для различных приложений, особое внимание уделяется путям проектирования современных систем информационно-коммуникационных технологий (ИКТ) на основе IoT и связанных с ними концептуальных архитектур, включая требования к сетям и протоколы. Учитывая большой объем возможностей IoT, высокоэффективные системы ИКТ, удовлетворяющие потребностям вертикальных отраслей, могут быть реализованы благодаря дополнительной разработке на основе архитектур IoT. Этот путь является перспективным с точки зрения эффективности и времени выхода на рынок.

Для поддержки такого подхода необходимо провести исследования архитектур IoT и SC&C, их функциональных возможностей, интерфейсов, протоколов, моделей данных, механизмов интеллектуального управления, механизмов контроля, технологий установления соединений, API и качества обслуживания/оценки пользователем качества услуг (QoE/QoS), в том числе на основе существующих Рекомендаций, включая МСЭ-Т Y.4000 /МСЭ-Т Y.2060.

### C.2 Вопросы

В рамках данного Вопроса рассматриваются архитектуры, включая их функциональные возможности, интерфейсы, протоколы, модели данных, механизмы интеллектуального управления, механизмы контроля, технологии установления соединений, API и качество обслуживания/оценку пользователем качества услуг (QoE/QoS) для IoT и "умных" устойчивых городов и сообществ (SSC&C), которые необходимы для построения архитектурных структур для взаимодействия с услугами и приложениями, а также с различными сетями и системами.

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

– Какие новые и пересмотренные Рекомендации необходимы для реализации архитектур IoT и SC&C?

– Какие технологии, включая сети, интерфейсы, функциональные возможности, механизмы управления, а также протоколы необходимы для архитектуры IoT и SC&C?

– Какие функциональные возможности технологий ИКТ, сигнализации и архитектур управления необходимы для поддержки услуг и/или приложений IoT и SC&C?

– Какие улучшения в существующих технологиях установления соединений, интерфейсах, функциональных возможностях, механизмах управления и протоколах необходимы для поддержки услуг и/или приложений межмашинного взаимодействия (M2M) в рамках IoT и SC&C?

– Какие требования к характеристикам технологий установления соединений необходимы для поддержки услуг и/или приложений IoT и SC&C?

– Какие механизмы достижения QoS/QoE и принципы измерения необходимы для IoT и SC&C?

− Сотрудничество с какими организациями по разработке стандартов (ОРС) будет необходимым для максимального увеличения синергии и согласования существующих стандартов?

### C.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– Разработка соответствующих Рекомендаций, Отчетов, руководящих указаний и т. д., касающихся:

• проведения исследований общих эталонных моделей IoT и потребностей вертикальных отраслей;

• разработки структур для определения базовых архитектурных композиций и описаний IoT и SC&C. Они будут основаны на определении требований к архитектуре, вытекающих из потребностей отрасли;

• определения объектов, их функций и эталонных точек, необходимых для поддержки приложений и услуг IoT;

• определения требований, на обеспечение которых направлены установление соединений и протоколы. Ожидается, что эти требования необходимо будет периодически уточнять, для того чтобы отражать развитие технологий, связанных с IoT, с учетом технологий установления соединений, механизмов управления (включая управление устройствами) и протоколов, разработанных МСЭ-Т и другими ОРС;

• разработки изменений и усовершенствований для внесения в требования к сигнализации, технологии установления соединений, механизмы управления (включая управление устройствами) и протоколы, которые позволят им соответствовать требованиям и архитектурам IoT и SC&C;

• определения требований к характеристикам технологий установления соединений, которые позволят им соответствовать требованиям IoT и SC&C;

• разработки механизмов достижения QoS и принципов его измерения, необходимых для IoT и SC&C;

• определения интерфейсов, для которых желательно обеспечить функциональную совместимость между различными сетевыми элементами IoT и для которых необходимо изучить подробные требования и разработать стандарты для протоколов;

• определения процедур взаимодействия с традиционными системами;

• разработки технологий, связанных с интеллектуальным контролем, которые будут обеспечивать поддержку приложений и услуг IoT для различных вертикальных отраслей и систем;

• определения механизмов для достижения функциональной совместимости архитектур IoT и SC&C.

– Обеспечение необходимого сотрудничества для совместной деятельности в этой области в рамках МСЭ, а также между МСЭ и ОРС, консорциумами и форумами.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК20 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=3/20>.

### C.4 Относящиеся к Вопросу

Направления деятельности ВВУИО

– C2, C3, C5, C6, C7, C8, C10

Цели в области устойчивого развития

– 9 и 11

Рекомендации

– Серия Y.4000

Вопросы

– Все Вопросы ИК20 МСЭ-T

Исследовательские комиссии

− Соответствующие исследовательские комиссии МСЭ-T (например, с учетом выполнения ими функции ведущей исследовательской комиссии), МСЭ-D и МСЭ-R

– Сигнализация и протоколы IoT будут разработаны в сотрудничестве с ИК11 МСЭ-T.

Другие органы

– ATIS

– IETF

– ЕТСИ

– oneM2M

– РГ10 ОТК1 ИСО/МЭК

– Объединенная целевая группа по "умным" городам МЭК/ИСО/МСЭ

– 3GPP/3GPP2

– IEEE

– W3C

– OCF

ВОПРОС D/20

Анализ и обработка данных, обмен и управление данными в IoT и SC&C, включая аспекты больших данных

(Продолжение Вопроса 4/20)

### D.1 Обоснование

Наблюдается рост спроса на соединенные города с повсеместно встроенными устройствами для повышения качества услуг интернета вещей (IoT) и умных городов и сообществ (SC&C). Развитие технологий IoT с использованием взаимосвязанных объектов помогает представить "умную среду" с автономной информационной инфраструктурой, с несколькими источниками данных и с более чем 50 млрд. устройств в экосистеме IoT и SC&C.

Традиционные инфраструктуры баз данных и архитектуры анализа информации сохраняют значимость, однако с возрастанием спроса на управление данными требуются особые возможности и пропускная способность для обеспечения обработки потоков различных и сложных данных из разных источников. Эти данные необходимо обрабатывать и управлять ими надлежащим образом, с тем чтобы безопасным и соответствующим требованиям политики образом повысить их ценность, дополняя их при этом данными из других источников информации.

Важно отметить, что любые дефекты в структуре обработки данных и управлении ими (DPM) могут существенно снизить качество услуг, создать риски, связанные с безопасностью, и препятствовать процессу городского планирования и принятия решений в целом.

В связи с вышесказанным для сред IoT и SC&C все чаще требуются определенные и комплексные структуры и руководящие принципы DPM, которые включают разумные меры для достижения многоуровневой ориентированной на данные парадигмы. Услуги и приложения, основанные на данных, будут обеспечиваться инструментами анализа данных, встроенными в экосистему данных с использованием появляющихся технологий (например, блокчейна, искусственного интеллекта, виртуальной копии и других) для поддержки IoT и SC&C. Таким образом, в рамках данного Вопроса предполагается определение и исследование характеристик формирующихся систем DPM с учетом аспектов больших данных в IoT и SC&C.

Внедрение осуществимых руководящих принципов и стандартов для DPM может сделать сбор, хранение и извлечение больших объемов данных быстрым и экономически эффективным при одновременном решении проблем, связанных со сложностью данных и управлением ими.

Принимая во внимание экосистему данных, которая влияет на различные заинтересованные стороны, в рамках работы над этим Вопросом предполагается разработать ряд Рекомендаций по эффективному DPM, анализу данных и обмену ими в IoT и SC&C.

### D.2 Вопросы

В рамках работы над данным Вопросом основное внимание будет уделено DPM, анализу данных и обмену ими в IoT и SC&C, включая аспекты больших данных.

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

– анализ существующих технологий, платформ, руководящих принципов и стандартов для DPM в соответствии с мандатом ИК20;

– архитектурные структуры для будущих экосистем, основанных на данных, и их применение для DPM и больших данных;

– вопросы анализа данных и обмена данными, связанные с разработкой эффективных и масштабируемых подходов к DPM;

– роль появляющихся технологий (например, блокчейна, искусственного интеллекта, виртуальной копии и других) в поддержке DPM;

– вопросы управления, безопасности и конфиденциальности в структурах DPM;

– доверенные данные и качество данных в структурах DPM, включая цифровую идентификацию и сертификацию;

– сотрудничество с организациями по разработке стандартов (ОРС) для максимального увеличения синергии и согласования существующих стандартов, касающихся данного направления работы.

### D.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– Разработка соответствующих Рекомендаций, Добавлений, Отчетов, руководящих указаний и т. д. по тематике DPM в IoT и SC&C, охватывающих:

• методологию построения концепции DPM на основе сценариев использования и анализа требований;

• цепочку создания стоимости данных, жизненный цикл данных, возможности и функциональные архитектуры для поддержки DPM в IoT и SC&C, включая аспекты больших данных;

• анализ данных и обмен данными для поддержки основанных на данных интеллектуальных услуг и приложений IoT и SC&C;

• инструменты, механизмы и стандартизированные интерфейсы для анализа данных и обмена данными;

• DPM, анализ данных и обмен данными с использованием появляющихся технологий (например, блокчейна, искусственного интеллекта, виртуальной копии и других) в IoT и SC&C;

• управление, безопасность, защиту конфиденциальности и управление рисками в IoT и SC&C;

• доверенные данные и управление качеством данных в IoT и SC&C.

– Обеспечение необходимого сотрудничества для совместной деятельности в этой области в рамках МСЭ, а также между МСЭ-Т и другими соответствующими ОРС, консорциумами и форумами.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК20 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=4/20>.

### D.4 Относящиеся к Вопросу

Направления деятельности ВВУИО

– C2, C3, C5, C6, C7, C8, C10, C11

Цели в области устойчивого развития

– 9, 10 и 11

Рекомендации

– Серия Y.4000 по IoT и "умным" городам и сообществам

– Серия Y.4000 по обработке данных и управлению данными (включая результаты работы ОГ-DPM МСЭ-T)

Вопросы

– Все Вопросы ИК20 МСЭ-T

Исследовательские комиссии

− Соответствующие исследовательские комиссии МСЭ-T (например, с учетом выполнения ими функции ведущей исследовательской комиссии), МСЭ-D и МСЭ-R

– Работа над данным Вопросом предполагает координацию с ИК13 МСЭ-Т по соответствующим аспектам больших данных.

Другие органы

– 3GPP

– Альянсы 5G (например, 5G AA, 5G ACIA и др.)

– BDVA

– BSI

– ЕТСИ

– Ассоциация GSM

– IEEE

– IETF

– ОТК 1 ИСО/МЭК

– Объединенная целевая группа по "умным" городам МЭК/ИСО/МСЭ

– OASC

– OCF

– OMA

– oneM2M

– OSG

– W3C

ВОПРОС E/20

Исследование появляющихся цифровых технологий,
терминологии и определений

(Продолжение Вопроса 5/20)

### E.1 Обоснование

Интернет вещей (IoT) способен изменить образ жизни людей и способ их взаимодействия с внешней средой, в особенности в "умных" городах и сообществах (SC&C). В связи с этим важно исследовать появляющиеся технологии и тенденции, которые будут способствовать данному изменению. Ожидается, что IoT окажет существенное воздействие на важнейшие инфраструктурные элементы городов, в том числе секторы транспорта, здравоохранения и энергетики, качество жизни и окружающую среду, а также на общество и экономику в целом. В силу своей повсеместной распространенности IoT находится в непосредственном взаимодействии со всеми прикладными областями и всеми странами, что оказывает непосредственное влияние на достижение Целей в области устойчивого развития.

В целях содействия обсуждениям и обеспечения общей базовой информации по соответствующим вопросам необходимы координация и унификация терминологии, связанной с IoT и SC&C. Было бы также целесообразно определить, исследовать и проанализировать появляющиеся цифровые технологии, которые имеют отношение к стандартизации IoT и/или SC&C. Работа над данным Вопросом должна стать каналом связи с исследовательским сообществом и, при необходимости, способствовать передаче появляющихся технологий для стандартизации и ускорять такую передачу. Данный Вопрос будет сосредоточен на темах, которые еще не рассматривались в рамках других Вопросов.

### E.2 Вопросы

Задачей этого Вопроса является сбор и разработка определений в целях содействия формированию общей терминологии для IoT и SC&C. Помимо этого, данный Вопрос может способствовать исследованию решений для обеспечения функциональной совместимости различных технологий и учету потребностей конечных пользователей, регуляторных органов и рынка. Принимая во внимание стремительное развитие сферы IoT, данный Вопрос может также способствовать выявлению и обсуждению соответствующих научных исследований и технологических наработок в этой области и доведению наиболее важных тем до сведения 20-й Исследовательской комиссии МСЭ-T (ИК20) и/или соответствующих Вопросов. Принимая во внимание стремительное развитие технологий IoT и сокращение времени выхода на рынок, предполагается, что работа над данным Вопросом будет способствовать взаимодействию с научно-исследовательским и инновационным сообществом для целей выявления появляющихся технологий, требующих стандартизации для глобального рынка и отрасли.

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

– Какие термины, определения, сокращения, буквенные обозначения и условные обозначения используются применительно к IoT и SC&С?

– Какие появляющиеся исследования и технологии, связанные с IoT и/или SC&C, могут быть стандартизованы?

– Какой вклад могут внести технологии IoT в достижение Целей в области устойчивого развития (ЦУР)?

– Какое воздействие оказывает внедрение IoT на деятельность человека и каким образом можно устранить соответствующие ограничения?

– Каким образом можно улучшить опыт взаимодействия конечного пользователя с IoT?

– Как IoT может соответствовать нормативным требованиям и как системы и компоненты IoT могут стандартизованно обмениваться информацией о своем соответствии требованиям нормативно-правовой базы?

– Каким образом IoT будет менять бизнес-модели и рыночную среду?

– Сотрудничество с какими организациями по разработке стандартов (ОРС) будет необходимым для максимального увеличения синергии и согласования существующих стандартов?

– Как взаимодействовать с широким сообществом IoT, включая его различные заинтересованные стороны, для поддержки глобальной стандартизации и функциональной совместимости?

### E.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– Разработка соответствующих Рекомендаций, Отчетов, руководящих указаний и т. д., касающихся:

• разработки, поддержания и совершенствования Рекомендаций по терминологии, связанной с IoT и SC&C;

• поддержания и совершенствования Рекомендаций 20-й Исследовательской комиссии;

• разработки в МСЭ-Т на основе сотрудничества в рамках других Вопросов ИК20 структур и дорожных карт для согласованного и скоординированного развития IoT, в том числе межмашинного взаимодействия и повсеместно распространенных сенсорных сетей;

• сотрудничества с исследовательскими комиссиями МСЭ-D и МСЭ‑R, а также другими региональными и международными организациями по разработке стандартов (ОРС), академическими организациями и отраслевыми форумами;

• разработки руководящих указаний, методик и примеров передового опыта в сфере IoT и SC&C для поддержки достижения Целей в области устойчивого развития (ЦУР) и предотвращения цифрового разрыва с развивающимися странами;

• разработки руководящих указаний, методик и примеров передового опыта в сфере IoT для поддержки соблюдения правовых норм, действующих в отношении систем и решений IoT, при соблюдении принципов стандартизации и функциональной совместимости;

• определения появляющихся технологий и соответствующих исследований в сфере IoT и SC&C, которые имеют отношение к задачам стандартизации;

• поддержания связей и развития сотрудничества с академическим, исследовательским и инновационным сообществом, а также с другими ОРС и отраслевыми форумами, в том числе с малыми и средними предприятиями (МСП), по проблематике IoT и SC&C;

• выявления на основе сотрудничества в рамках других Вопросов ИК20 новых направлений работы, связанных с IoT и SC&C, а также взаимодействия с соответствующими ИК МСЭ-Т и другими ОРС и форумами в целях проведения исследований по этим определенным направлениям работы;

– Обеспечение необходимого сотрудничества для совместной деятельности в этой области в рамках МСЭ, а также между МСЭ-Т и другими соответствующими ОРС, консорциумами и форумами.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК20 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=5/20>.

### E.4 Относящиеся к Вопросу

Направления деятельности ВВУИО

– C1, C6, C11

Цели в области устойчивого развития

– 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 и 17

Рекомендации

– Y.4050/Y.2069

Вопросы

– Все Вопросы ИК20 МСЭ-T

Исследовательские комиссии

− Соответствующие исследовательские комиссии МСЭ-T (например, с учетом выполнения ими функции ведущей исследовательской комиссии), МСЭ-D и МСЭ-R

– Группа Докладчика КГСЭ по стратегии стандартизации (ГД-StdsStrat)

– Комитет МСЭ по стандартизации терминологии

Другие органы

– МЭК

– ISO

– Объединенная целевая группа по "умным" городам МЭК/ИСО/МСЭ

– IEEE

– IETF

– Форум IPv6

– Форум IoT

– Лаборатория IoT

ВОПРОС F/20

Безопасность, конфиденциальность, доверие и идентификация для IoT и SC&C

(Продолжение Вопроса 6/20)

### F.1 Обоснование

В процессе движения к информационному обществу возрастает количество случаев кибератак, киберпреступлений, потери репутации и доверия. Инфраструктура ИКТ будет развиваться с целью предоставления конвергентных услуг и приложений путем размещения множества датчиков интернета вещей (IoT) и связанных с IoT систем. Кроме того, в мире происходит развитие "умных" городов. Многие заинтересованные стороны из различных отраслей вовлечены в создание будущих конвергентных и интеллектуальных услуг, которые должны быть развернуты с использованием инфраструктуры ИКТ. Эта разнородная среда, несмотря на обещание больших перспектив в направлении предоставления услуг и приложений, а также в отношении способов управления, администрирования и технического обслуживания, обладает очень широким спектром характерных для сектора рисков и векторов угроз. Последствия для безопасности, конфиденциальности[[1]](#footnote-1)1 и общего доверия к использованию, внедрению и распространению IoT, а также устройств, систем, услуг, приложений и платформ для "умных" городов могут препятствовать развитию их рынка в целом. Поэтому важно принимать во внимание проблемы безопасности и конфиденциальности на этапе проектирования продуктов и систем, которые создаются для использования в IoT, что также известно как соблюдение принципа "конфиденциальность и безопасность на этапе проектирования", который подчеркивает, что защита должна встраиваться в информационные технологии, практику бизнеса, системы, процессы, физические конструкции и сетевую архитектуру.

Соответствие требованиям по безопасности и конфиденциальности играет фундаментальную роль в среде IoT и SC&C. Эти требования включают конфиденциальность и аутентификацию данных, управление доступом в рамках сети IoT, доступность, целостность данных, конфиденциальность и доверие между пользователями и вещами, предотвращение отказа от авторства.

Некоторые меры безопасности не всегда могут быть непосредственно применены к технологиям IoT. Помимо этого, из-за большого количества взаимно соединяемых устройств возникают проблемы масштабируемости, поэтому требуется гибкая архитектура, способная справиться с угрозами безопасности в такой среде. Инфраструктура ИКТ должна быть надежной, безопасной конфиденциальной и обеспечивающей доверие. Таким образом, обеспечение безопасности, конфиденциальности и доверия в среде IoT является одним из нерешенных вопросов стандартизации, которым занимается ИК20 МСЭ‑T.

С другой стороны, различные технологии идентификации всегда рассматривались как важные благоприятствующие технология для внедрения IoT. И физическим устройствам (таким, как маркированные объекты и продукты, сенсорные устройства), и виртуальным объектам (таким, как вычислительные процессы и программное обеспечение) можно было бы присвоить (или уже присвоен) идентификатор, чтобы их можно было идентифицировать и отличать от других. Важно обеспечить, чтобы каждый предмет был адресуемым и идентифицируемым, для того чтобы можно было решать проблемы конфиденциальности, безопасности, доверия и досягаемости сети при развертывании IoT.

Принимая во внимание разнообразие устройств, систем, услуг и приложений в IoT и SC&C, необходимо разработать модели доверия, которые гарантируют, что все физические и виртуальные объекты, вовлеченные в процесс, будут достаточно надежными, чтобы быть частью среды IoT и SC&C. Такие модели должны быть интегрированы в архитектуры IoT и SC&C, а также должны быть определены правила для обеспечения реализации доверенных систем IoT. Архитектуры безопасности и надежности должны быть существенной частью любых архитектур E2E, разработанных для вертикальных отраслей и сценариев использования IoT и SC&C.

Помимо этого, внедрение новых технологий, таких как блокчейн, большие данные, квантовые вычисления, машинное обучение и искусственный интеллект (ИИ) может сыграть важную роль в разработке передовых экономически эффективных мер и механизмов для создания такой доверенной среды в областях IoT и SC&C.

Все вышеперечисленные требования должны быть тщательно проанализированы для различных вертикальных отраслей и сценариев использования IoT, которые могут быть сопряжены со особыми дополнительными требованиями в силу своей специфики и лежащих в их основе стандартов, используемых для устройств, систем, приложений, протоколов, платформ и услуг IoT и SC&C.

### F.2 Вопросы

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

– Каковы возможные угрозы компрометации аутентичности, конфиденциальности, целостности, предотвращения отказа от авторства и доступности устройств, систем, приложений, протоколов, платформ и услуг IoT и SC&C?

– Что необходимо для уменьшения рисков и угроз, выявляемых в системах и услугах IoT и SC&C, и для противодействия таким рискам и угрозам?

– Какие существуют системы идентификации, соответствующие требованиям IoT и SC&C, включая требования безопасности, конфиденциальности и доверия?

– Каковы требования и механизмы для защиты и предотвращения раскрытия информации, касающейся предметов?

– Как технологии аутентификации могут работать с идентификационными системами?

– Каким образом меры безопасности могут быть применены в устройствах IoT для защиты идентичности, конфиденциальности и безопасности системы, учитывая, что среда и ресурсы устройства могут быть ограничены?

– Какие технические меры необходимы для обеспечения защиты конфиденциальности в приложениях, услугах и платформах SC&C? Каким образом можно обеспечить и поддерживать доверие к использованию таких систем?

– Какие меры могут быть приняты для предотвращения компрометации и защиты целостности и конфиденциальности систем, приложений, платформ и услуг IoT?

– Как создать доверенную среду в устройствах, системах, приложениях, протоколах, платформах и услугах IoT и SC&C?

– Как обеспечить безопасность, конфиденциальность и достоверность данных, связанных с IoT и SC&C, а также соответствующих платформ данных?

– Как технологии и механизмы, основанные на блокчейне, могут поддерживать безопасность и достоверность в IoT и SC&C?

– Как использовать технологии машинного обучения и искусственного интеллекта (ИИ) для поддержки защищенной функциональной совместимости и достоверности в IoT и SC&C?

– Как квантовые технологии могут обеспечить безопасность и достоверность в IoT & SC&C?

– Как применять технологии больших данных для повышения безопасности и достоверности в IoT & SC&C?

– Как инфраструктура открытого ключа может усовершенствовать механизмы аутентификации и достоверность связи в IoT и SC&C?

– Какие меры могут быть разработаны для обеспечения доступности и переносимости данных в платформах, системах и услугах IoT и SC&C?

– Какие варианты или меры доступны для идентификации объектов IoT для SC&C, включая объекты не на базе IP и веб в разнородных системах IoT?

– Какие системы и механизмы идентификации могут быть использованы для поддержки IoT и SC&C?

– Каким образом механизмы идентификации могут поддерживать функциональную совместимость в области IoT и SC&C и снижать риски?

– Как обеспечить безопасность и достоверность взаимодействия с помощью интерфейсов прикладного программирования (API)?

– Какие варианты и механизмы могут быть использованы для регистрации идентификаторов IoT и управления ими, когда это необходимо?

– Какие технические меры необходимы для обнаружения идентичности?

– Сотрудничество с какими организациями по разработке стандартов (ОРС), консорциумами и форумами будет необходимым для максимального увеличения синергии и согласования существующих стандартов

### F.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– Разработка соответствующих Рекомендаций, Отчетов, руководящих указаний и т. д., касающихся:

• аутентичности, конфиденциальности, целостности, предотвращения отказа от авторства и готовности устройств, систем, приложений, протоколов, платформ и услуг IoT;

• обеспечения безопасности и достоверности в IoT как в инфраструктуре ИКТ, так и в будущих разнородных конвергентных средах услуг;

• обеспечения безопасности и достоверности в услугах и приложениях IoT для конвергентных сред между заинтересованными сторонами из различных отраслей;

• требований по снижению рисков и угроз, выявленных в системах и услугах IoT и SC&C;

• использования конструкций безопасности в системах IoT для защиты идентификатора, конфиденциальности и безопасности системы;

• технических мер по предотвращению угроз и защите целостности и конфиденциальности систем, приложений, платформ и услуг IoT;

• технических мер, необходимых для обеспечения защиты конфиденциальности в приложениях, услугах и платформах SC&C;

• выявления потенциальных рисков, связанных с управлением, администрированием, техническим обслуживанием и предоставлением услуг в SC&C;

• уменьшения рисков, связанных с управлением, администрированием, обслуживанием и предоставлением услуг в SC&C;

• обеспечения доступности и переносимости данных в платформах, системах и услугах IoT и SC&C;

• использования наименования, адресации и идентификации при развертывании IoT и SC&C;

• обнаружения идентичности и управления идентичностью в IoT и SC&C;

• методов достижения достоверности в устройствах, системах, приложениях, протоколах, платформах и услугах IoT и SC&C;

• безопасности и достоверности при использовании интерфейсов прикладного программирования (API);

• технологий и механизмов на основе блокчейна для поддержки безопасности и достоверности в IoT & SC&C;

• технологий машинного обучения и искусственного интеллекта (ИИ) для поддержки защищенной функциональной совместимости и достоверности в IoT и SC&C;

• механизмов квантовых вычислений для поддержки безопасности и достоверности в IoT и SC&C;

• технологий работы с большими данными для повышения безопасности и достоверности в IoT и SC&C;

• архитектур безопасности для IoT и SC&C;

• безопасности, конфиденциальности и достоверности данных и соответствующих платформ в IoT и SC&C.

– Обеспечение необходимого сотрудничества для совместной деятельности в этой области в рамках МСЭ, а также между МСЭ-Т и ОРС, консорциумами и форумами.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК20 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=6/20>.

### F.4 Относящиеся к Вопросу

Направления деятельности ВВУИО

– C5

Цели в области устойчивого развития

– 11 и 17

Рекомендации

– Серия Y и другие Рекомендации, касающиеся вопросов безопасности, конфиденциальности, доверия и идентификации.

Вопросы

– Все Вопросы ИК20 МСЭ-T

Исследовательские комиссии

− Соответствующие исследовательские комиссии МСЭ-T (например, с учетом выполнения ими функции ведущей исследовательской комиссии), МСЭ-D и МСЭ-R

– Работа над данным Вопросом предполагает координацию с ИК2 и ИК17 МСЭ-Т по аспектам идентификации в IoT в соответствии с кругом ведения каждой исследовательской комиссии

– Работа над данным Вопросом предполагает координацию с ИК17 МСЭ-Т по аспектам безопасности, конфиденциальности и доверия, связанным с IoT и SC&C, в соответствии с кругом ведения исследовательской комиссии

Другие органы

– ЕТСИ

– ENISA

– AIOTI

– IEEE

– 3GPP

– W3C

– ОТК1 ИСО/МЭК

– Объединенная целевая группа по "умным" городам МЭК/ИСО/МСЭ

– IETF

– OASIS

– oneM2M

ВОПРОС G/20

Анализ и оценка "умных" устойчивых городов и сообществ

(Продолжение Вопроса 7/20)

### G.1 Обоснование

Комплексные стратегии реализации проектов "умных" устойчивых городов и сообществ (SSC&C) появляются во всем мире, интегрируя информационно-коммуникационные технологии (ИКТ) во все аспекты городского планирования и функционирования городов. В ходе этого процесса ИКТ, в особенности интернет вещей (IoT) и другие появляющиеся технологии, повышают эффективность функционирования городов, обеспечивая использование соответствующей информации из различных источников путем проведения надлежащего анализа данных. Это позволяет муниципалитетам, сообществам и гражданам принимать более обоснованные решения и способствует более эффективной интеграции городских услуг и сотрудничеству между различными секторами.

На данном этапе важно иметь возможность измерять качественные показатели различных предприятий SC&C. Один из таких подходов основывается на ключевых показателях деятельности (KPI), которые облегчают мониторинг прогресса, достигнутого при переходе к SC&C, включая реализацию IoT в таких конкретных секторах, как защита окружающей среды, обеспечение безопасности, транспорт, здравоохранение, образование и коммунальные службы.

Желательно, чтобы города могли количественно оценивать свои достижения в соответствии со своими целями. Таким образом, используя эти показатели, города и их заинтересованные стороны могут также объективно оценивать степень, с которой они могут восприниматься как более "умные" и более устойчивые города.

### G.2 Вопросы

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

– Каковы общие принципы, которые следует использовать для разработки методики оценки использования ИКТ, а также воздействия ИКТ на устойчивость городов и уровень их интеллектуализации.

– Индекс "умных" устойчивых городов для использования во всем мире в различных странах и регионах.

– Полезность различных методик (измерение, статистическая выборка, исследования конкретных случаев, передовой опыт и пр.) для различных стран и регионов.

– Лучшие методы сбора надежных данных, учитывающие изменения этих данных во времени.

– Как оценивать достижение целей устойчивого развития (ЦУР) в "умном" городе?

– Как измерять и оценивать результаты работы города по конкретному направлению и электронные/умные услуги в отношении определенных отраслевых (или вертикальных) показателей, таких как показатели открытых данных, показатели электронного здравоохранения, показатели коммунальных услуг и пр.

– Как оценить устойчивость города к внешним воздействиям.

– Сотрудничество с какими организациями по разработке стандартов (ОРС) будет необходимым для максимального увеличения синергии и согласования существующих стандартов?

### G.3 Задачи

К числу задач, наряду с прочими, относятся следующие:

– Разработка соответствующих Рекомендаций, Отчетов, руководящих указаний и т. д., касающихся:

• предоставления руководств и структурированных методов для городов в целях содействия установлению приоритетов по инициативам, а также для оценки уровня развития "умных" и устойчивых городов;

• разработки методик оценки достижения ЦУР городами с учетом общих принципов и критериев оценки воздействия ИКТ;

• определения методов сбора и вычисления надежных данных для использования в модели оценки;

• разработки методов и структур для измерения и оценки показателей деятельности города по конкретным направлениям и электронных/интеллектуальных услуг с учетом определенных отраслевых показателей;

• разработки методов и структур для оценки устойчивости "умного" города к внешним воздействиям;

• подготовки отчета по глобальному индексу "умных" устойчивых городов.

• подготовки отчета по показателям деятельности города, чтобы оказать помощь городам в достижении ЦУР.

– Обеспечение необходимого сотрудничества для совместной деятельности в этой области в рамках МСЭ, а также между МСЭ-Т и ОРС, учреждениями ООН, консорциумами и форумами.

Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК20 по адресу: <https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=7/20>.

### G.4 Относящиеся к Вопросу

Направления деятельности ВВУИО

– C2, C3, C6, C7, C8, C10, C11

Цели в области устойчивого развития

– 3, 6, 7, 9, 11 и 13

Рекомендации

– Все соответствующие Рекомендации и добавления серии Y.4000

Вопросы

– Все Вопросы ИК20 МСЭ-T

Исследовательские комиссии

− Соответствующие исследовательские комиссии МСЭ-T, МСЭ-D и МСЭ-R

Другие органы

– IETF

– Открытый альянс подвижной связи (OMA)

– Открытый геопространственный консорциум (OGC)

– IEEE

– ATIS

– ТК Smart M2M ЕТСИ

– TC10 CCSA

– oneM2M

– ПК41 ОТК1 ИСО/МЭК, РГ11 ОТК1 ИСО/МЭК

– Объединенная целевая группа по "умным" городам МЭК/ИСО/МСЭ

– Ассоциация GSM

– 3GPP/3GPP2

– W3C

– Организация по развитию стандартов структурированной информации (OASIS)

– Группа управления объектами (OMG)

– Промышленный консорциум интернета (IIC)

– Альянс промышленного интернета (AII)

– Альянс для инноваций в IoT (AIOTI)

– Фонд "Открытые соединения" (OCF)

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

1. 1 Соответствует Резолюции 2 (Пересм. Хаммамет, 2016 г.) ВАСЭ. [↑](#footnote-ref-1)