|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Всемирная ассамблея по стандартизации электросвязи (ВАСЭ-16) Хаммамет, 25 октября – 3 ноября 2016 года** | | C:\Users\gaspari\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\logos-02.png |
|  | |  | |
| **ПЛЕНАРНОЕ ЗАСЕДАНИЕ** | | **Дополнительный документ 32 к Документу 43-R** | |
|  | | **11 октября 2016 года** | |
|  | | **Оригинал: английский** | |
|  | | | |
| Администрации арабских государств | | | |
| предложения и мнения о структуре 20-й исследовательской комиссии МСЭ-T | | | |
|  | | | |
|  | | | |

|  |  |
| --- | --- |
| **Резюме**: | Администрации арабских государств предлагают добавить два новых Вопроса и рассмотреть структуру 20-й Исследовательской комиссии МСЭ-T с целью укрепления роли ИК20 с учетом рассмотрения представленных настоящей Ассамблее Документов 22 и 21, в частности раздела, относящегося к Замечаниям, касающимся будущей работы ИК20. |

Обсуждение

– На своем собрании в июне 2015 года Консультативная группа по стандартизации электросвязи (КГСЭ) решила создать новую 20-ю Исследовательскую комиссию МСЭ-Т под названием "IoT и его приложения, включая "умные" города и сообщества". Круг ведения, структура ИК20 и текст Вопросов были утверждены на собрании КГСЭ (июнь 2015 г.), и их можно найти в Документе [TD/322(Rev.3)](http://www.itu.int/md/T13-TSAG-150602-TD-GEN-0322/en).

– Структура ИК20 была утверждена на собрании КГСЭ в июне 2015 года. В нее были внесены поправки на первом собрании ИК20, состоявшемся 19–23 октября 2015 года. ИК20 согласовала структуру, содержащуюся в Документе [TD/003(Rev.5)(GEN/20)](http://www.itu.int/md/T13-SG20-151019-TD-GEN-0003/en), которая была представлена КГСЭ в феврале 2016 года.

КГСЭ на своем собрании в феврале 2016 года согласовала следующие аспекты, которые представлены в ее отчете об этом собрании:

– функция ведущей исследовательской комиссии ИК20 МСЭ-T по темам "Интернет вещей (IoT) и его приложения" и "«Умные» города и сообщества (SC&C)";

– обновленный текст шести Вопросов ИК20, содержащийся в Приложении C к Дополнению 1 Заявления о взаимодействии ИК20 МСЭ-T ([TD/368](http://www.itu.int/md/T13-TSAG-160201-TD-GEN-0368/en));

– изменения в мандате и сфере деятельности JCA-IoT и SC&C при условии, что формулировка первой цели JCA будет изменена следующим образом: "…и осуществлять взаимодействие с МСЭ-R…".

В настоящем вкладе предлагается добавить два новых Вопроса и внести изменение в структуру ИК20 с целью расширить и укрепить роль ИК20 для выполнения ее мандата.

# 1 Предлагаемые два новых Вопроса

ARB/43A32/1

Новый Вопрос 2/20 "Анализ и оценка "умных" городов и сообществ"

В соответствии с мандатом, полученным от КГСЭ ИК20 в качестве ведущей Исследовательской комиссии по "умным" городам и сообществам, и принимая во внимание работу, переданную ИК20 из 5-й Исследовательской комиссии МСЭ-Т, авторы настоящего вклада предлагают создать новый Вопрос "Анализ и оценка "умных" городов и сообществ".

вопрос 2/20

Анализ и оценка "умных" городов и сообществ

### 1 Обоснование

Комплексные стратегии создания "умных" городов и сообществ (SC&C) появляются во всем мире в ответ на проблемы, возникающие в связи со стремительной урбанизацией. К их числу относится интеграция информационно-коммуникационных технологий (ИКТ) во все аспекты городского планирования и функционирования городов. В ходе этого процесса ИКТ, в особенности интернет вещей (IoT), повышают эффективность функций городов, обеспечивая сбор надлежащей информации и соединяя множество различных сфер. Это позволит соответствующим муниципалитетам, сообществам и гражданам принимать более обоснованные решения, способствуя тем самым интеграции городских услуг и сотрудничеству между различными секторами.

На этом этапе важно уметь 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, а также в таких конкретных секторах, как защита окружающей среды, здравоохранение, образование, коммунальные службы.

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

### 2 Вопрос

Необходимые для рассмотрения темы исследования включают, в том числе:

– Каковы общие принципы, которые следует использовать для разработки методики оценки использования ИКТ, а также воздействия ИКТ на устойчивость городов?

– Каковы формулы для расчета индекса, характеризующего "умные" устойчивые города, для их всемирного использования?

– Как осуществлять сбор надежных данных, в частности данных, которые весьма существенно влияют на результаты? Каким образом учитывать динамику данных во времени?

– Как оценивать методику (измерения, статистической выборки, исследований конкретных ситуаций и т. д.), включая различные региональные или национальные аспекты?

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

– Как измерять характерные для города качественные показатели в отношении определенных для сектора показателей, таких как индикаторы открытых данных, показатели, связанные с электронным здравоохранением, показатели коммунальных служб и т. д.

– Как анализировать качество услуг электронного здравоохранения? Как модернизировать системы электронного здравоохранения с целью их адаптации к будущим технологиям по результатам анализа?

– Сотрудничество с какими организациями по разработке стандартов (ОРС) будет необходимым для максимального увеличения синергии и согласования существующих стандартов, касающихся оценки и анализа SC&C?

### 3 Задачи

Задачи включают, в том числе:

– Разработку Рекомендаций по методике оценки ЦУР городов с учетом общих принципов, критериев оценки воздействия ИКТ.

– Разработку Рекомендаций по осуществлению сбора и расчета надежных приближенных данных для включения в модели оценки.

– Разработку Рекомендаций по методике измерения в целях измерения характерных для города качественных показателей относительно определенных для сектора показателей.

– Разработку справочников, содержащих необходимые ссылки на имеющиеся базы данных, которые касаются общих профилей SC&C.

– Разработку справочников для предоставления отчетов о глобальном индексе "умных" устойчивых городов.

– Разработку руководящих указаний и примеров передового опыта по представлению качественных показателей о городе с целью оказания помощи городам в достижении ЦУР.

– Координирование деятельности с другими исследовательскими комиссиями и другими ОРС, а также с другими учреждениями ООН на регулярной основе в целях обеспечения эффективного сотрудничества.

ПРИМЕЧАНИЕ. – Информация о текущем состоянии работы по этому Вопросу содержится в программе работы ИК20 по адресу: <http://www.itu.int/ITU-T/workprog/wp_search.aspx?Q=xx/20>.

### 4 Относящиеся к Вопросу

Рекомендации:

– Серия Y.4000, включая Y.4900/L.1600, Y.4901/L.1601, Y.4902/L.1602 и Y.4903/L.1603

Вопросы:

– Все Вопросы ИК20

Исследовательские комиссии:

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

Другие органы:

– CEN-CENELEC-ЕТСИ, Группа по координации "«Умные» устойчивые города и сообщества" (SSCC-CG)

– ТК EE ЕТСИ

– ТК Smart M2M ЕТСИ

− SEG1 МЭК

− ТК111 МЭК

– OneM2M

– Сообщество "умных" городов IEEE

− ОТК1/РГ11 ИСО/МЭК

− ТК268/СК1 ИСО

– SAG ИСО − IIC (Промышленный консорциум интернета)

ARB/43A32/2

Новый Вопрос 3/20 "Безопасность, конфиденциальность, доверие и идентификация"

В соответствии с мандатом, полученным ИК20 от КГСЭ, на исследование безопасности, конфиденциальности, доверия и идентификации систем, услуг и приложений IoT и "умных" городов и сообществ (SCC), и принимая во внимание работу и исследования, выполняемые в рамках Вопросов 1/20, 4/20, 5/20 и 6/20, авторы настоящего вклада предлагают создать отдельный Вопрос "Безопасность, конфиденциальность, доверие и идентификация" для услуг и приложений, с учетом работы и исследований, предпринимаемых в рамках Вопросов 4/20, 5/20 и 6/20.

ВОПРОС 3/20

Безопасность, конфиденциальность, доверие и идентификация

### 1 Обоснование

В процессе движения к информационному обществу возрастает количество случаев кибератак, киберпреступлений, потери репутации и доверия. Инфраструктура ИКТ будет развиваться с целью предоставления будущих 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 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 реализовать принцип "конфиденциальность и безопасность на этапе проектирования", подчеркивающий, 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. Традиционные контрмеры безопасности не могут напрямую применяться к технологиям IoT из-за применения различных стандартов и стеков протоколов связи, в дополнение к различной требуемой конкретной компетентности в области знаний. Кроме того, из-за большого количества взаимно соединяемых устройств возникают проблемы масштабируемости, поэтому требуется гибкая архитектура, способная справиться с угрозами безопасности в такой динамичной среде. Будущая инфраструктура ИКТ должна быть надежной, безопасной конфиденциальной и, в достаточной степени, обеспечивающей доверие. Поэтому обеспечение безопасности и доверия для IoT является одной из нерешенных проблем стандартизации ИК20 МСЭ-T.

С другой стороны, технология идентификации всегда рассматривалась как важная благоприятствующая технология для внедрения IoT. И физическим устройствам (таким, как маркированные объекты и продукты, сенсорные устройства), и виртуальным объектам (таким, как вычислительные процессы, программное обеспечение) можно было бы присвоить идентификатор, чтобы их можно было идентифицировать и отличать от других. Поскольку какой-либо предмет состоит из других предметов, очень важно обеспечить, чтобы каждый предмет был адресуемым и идентифицируемым, для того чтобы можно было решать проблемы адресации, конфиденциальности, безопасности, доверия и досягаемости сети при развертывании IoT.

### 2 Вопрос

В настоящем Вопросе рассматриваются темы безопасности, конфиденциальности, обеспечения доверия, наименования, адресации и идентификации систем, услуг, приложений и протоколов IoT.

Необходимые для рассмотрения темы исследования включают, в том числе:

– Каковы возможные угрозы компрометации аутентичности, конфиденциальности, целостности, предотвращения отказа от авторства и доступности устройств, систем, приложений, протоколов, платформ и услуг, независимо от трудности и стоимости осуществления атаки, реализующей конкретную угрозу?

– Каковы оценки вероятности различных атак и потенциальной выгоды для атакующего какую-либо систему IoT/SC&C? Каков оцениваемый ущерб для атакуемой стороны?

– Каковы требования, необходимые для уменьшения рисков и угроз, выявляемых в устройствах, системах, приложениях, протоколах, платформах и услугах IoT и SC&C, и для противодействия им?

– Каковы системы идентификации, необходимые для удовлетворения требованиям IoT, включая требования безопасности, конфиденциальности и доверия?

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

– Каким образом можно интегрировать защищенное управление полномочиями в системы идентификации?

– Каким образом можно интегрировать технологии аутентификации в системы идентификации?

– Каким образом можно применить в устройствах IoT традиционные меры по обеспечению целостности, доступности, аутентичности, предотвращения отказа от авторства в целях защиты идентичности, конфиденциальности и безопасности системы, учитывая ограниченность ресурсов устройств с точки зрения энергии, пространства, памяти, полосы пропускания и возможности установления соединений?

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

– Каким образом можно предотвратить незаконное отслеживание, профилирование и незаконную обработку систем, приложений, платформ и услуг IoT?

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

– Каким образом можно рассматривать подключенные не на базе IP и/или не на базе веб объекты в смешанных разнородных системах IoT?

– Каким образом можно использовать семантическую функциональную совместимость в качестве механизма идентификации объекта? В чем заключаются риски, связанные с ложной идентификацией?

– Как осуществляется регистрация наименований IoT и управление ими?

– Какие технические меры необходимы для обнаружения идентичности? Какие атрибуты потребуются регистру идентификации, чтобы поддерживать идентификацию предметов и интеграцию систем?

– Как устройства предотвратят имитацию других устройств, с которыми они обмениваются данными? Как устройства, генерирующие, обрабатывающие, хранящие или извлекающие личные, чувствительные, конфиденциальные или секретные данные, могут обнаружить и предотвратить мошенническое использование?

### 3 Задачи

Задачи включают, в том числе:

– Разработку Рекомендаций по обеспечению аутентичности, конфиденциальности, целостности, предотвращения отказа от авторства и готовности устройств, систем, приложений, протоколов, платформ и услуг IoT.

– Разработку Рекомендаций по обеспечению безопасности и доверия к IoT как в рамках инфраструктуры ИКТ (например, так называемого уровня инфраструктуры), так и будущей неоднородной среды конвергированных услуг (например, так называемого уровня услуг).

– Разработку Рекомендаций по обеспечению безопасности и доверия к услугам и приложениям IoT для конвергированной среды среди многих заинтересованных сторон других отраслей промышленности (например, использование инфраструктуры ИКТ для сетей передачи электроэнергии)

– Разработку Рекомендаций по требованиям, необходимым для уменьшения рисков и угроз, выявляемых в устройствах, системах, приложениях, протоколах, платформах и услугах IoT и SC&C.

– Разработку Рекомендаций по использованию традиционных моделей обеспечения целостности, доступности, аутентичности, предотвращения отказа от авторства в системах IoT для защиты идентичности, конфиденциальности и безопасности системы.

– Разработку Рекомендаций по техническим мерам по предотвращению незаконного отслеживания, профилирования и незаконной обработки систем, приложений, платформ и услуг IoT.

– Разработку Рекомендаций по техническим мерам, протоколам и системам, необходимым для обеспечения защиты конфиденциальности в приложениях, услугах и платформах SC&C.

– Разработку руководящих указаний по выявлению потенциальных рисков, связанных с различными операциями по управлению, администрированию, техническому обслуживанию и предоставлению услуг в SC&C.

– Разработку руководящих указаний о том, как уменьшить риски, связанные с различными операциями по управлению, администрированию, техническому обслуживанию и предоставлению услуг в SC&C.

– Разработку Рекомендаций по обеспечению доступности и переносимости данных в платформах, системах и услугах IoT и SC&C.

– Разработку Рекомендаций по использованию наименования и идентификации при развертывании IoT и SC&C.

– Разработку Рекомендаций по обнаружению идентичности в IoT.

– Разработку Рекомендаций по управлению определением идентичности в IoT.

– Разработку Рекомендаций по наименованию и адресации в приложениях и услугах IoT/SC&C.

– Координация на регулярной основе деятельности с другими ИК и ОРС, а также с другими учреждениями системы ООН для достижения эффективного сотрудничества.

### 4 Относящиеся к Вопросу

Рекомендации:

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

Вопросы:

– Все Вопросы ИК20

Исследовательские комиссии:

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

Другие органы:

– ОТК1 ИСО/МЭК

– Фонд DONA

– ETF

– OASIS

– OneM2M

# 2 Предлагаемые изменения структуры ИК20

ARB/43A32/3

В течение последнего исследовательского периода ИК20 провела три собрания, на которых присутствовало большое количество участников. Работа, проводимая ИК20, оказалась весьма продуктивной: было получено 314 вкладов, создано несколько направлений работы и утверждено нескольких Рекомендаций.

Кроме того, ввиду возможного дублирования работы между РГ 1/20 (Интернет вещей) и РГ 2/20 ("Умные" города и сообщества) ИК20, было проведено несколько совместных собраний Вопросов, поскольку темы и/или вклады относились к нескольким Вопросам. Поэтому, авторы настоящего вклада предлагают пересмотреть и реорганизовать структуру ИК20, при понимании, что она будет отражать продолжение работы и сохранение мандатов ИК20 предыдущего исследовательского периода, как представлено в следующей таблице.

Предлагаемые изменения в структуре 20-й Исследовательской комиссии МСЭ-T

| Вопросы ИК20 | Название |
| --- | --- |
| **PLEN** |  |
| **Рабочая группа 1** |  |
| Вопрос 1/20 | Исследования и появляющиеся технологии, включая терминологию и определения |
| Вопрос 2/20 | Анализ и оценка "умных" городов и сообществ |
| Вопрос 3/20 | Безопасность, конфиденциальность, доверие и идентификация |
| **Рабочая группа 2** |  |
| Вопрос 4/20 | Требования, возможности, вертикальные сектора и сценарии использования |
| Вопрос 5/20 | Структуры, архитектуры и протоколы |
| Вопрос 6/20 | Услуги, приложения, вычисления и обработка данных |
| **Рабочая группа 3** |  |
| Вопрос 7/20 | Инфраструктура, возможность установления соединений, сети и функциональная совместимость |
| Вопрос 8/20 | Управление, контроль и рабочие характеристики |

# 3 Резюме предложений

1) Создать новый исследуемый Вопрос 2/20 "Анализ и оценка "умных" городов и сообществ".

2) Создать новый исследуемый Вопрос 3/20 "Безопасность, конфиденциальность, доверие и идентификация".

3) Изменить структуру ИК20, как показано в Документе ARB/043A32/3, в целях обеспечения большей синергии в деятельности между Вопросами ИК20, ограничения любого возможного дублирования между Вопросами и получения более надежной, целенаправленной и организованной структуры.

4) Просить ВАСЭ-16 обсудить и рассмотреть предлагаемую общую структуру и утвердить новые предлагаемые Вопросы.

5) Просить ВАСЭ-16 поручить ИК20 окончательно оформить эту структуру на своем первом собрании после ВАСЭ-2016 и разработать соответствующий текст для остальных вопросов (Вопрос 1/20, Вопрос 4/20, Вопрос 5/20, Вопрос 6/20, Вопрос 7/20 и Вопрос 8/20) с учетом итогов работы настоящей Ассамблеи.

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