|  |  |
| --- | --- |
| **Всемирная ассамблея по стандартизации  электросвязи (ВАСЭ-20) 1−9 марта 2022 года** |  |
|  |  |
| **ПЛЕНАРНОЕ ЗАСЕДАНИЕ** | Документ 19-R |
|  | **Декабрь 2021 года** |
|  | **Оригинал: английский** |
|  | |
| 17-я Исследовательская комиссия МСЭ-Т | |
| Безопасность | |
| ОТЧЕТ ИК17 МСЭ-Т ВСЕМИРНОЙ АССАМБЛЕЕ ПО СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ (васэ-20): ЧАСТЬ I – общая информация | |
|  | |

|  |  |  |
| --- | --- | --- |
| **Резюме**: | В настоящем вкладе содержится отчет 17-й Исследовательской комиссии МСЭ-Т для ВАСЭ-20 о деятельности в исследовательском периоде 2017−2021 годов. | |
| **Для контактов**: | г-н Хён-Юл Юм Председатель ИК17 МСЭ-Т Корея (Республика) | Эл. почта: [hyyoum@sch.ac.kr](mailto:hyyoum@sch.ac.kr) |

**Примечание БСЭ**:

Отчет 17-й Исследовательской комиссии для ВАСЭ-20 представлен в следующих документах:

Часть I: **Документ 19** – Общая информация

Часть II: **Документ 20** – Вопросы, предлагаемые для исследования в течение исследовательского периода 2021−2024 годов

СОДЕРЖАНИЕ

**Стр**.

[1 Введение 4](#_Toc95234802)

[1.1 Сфера ответственности 17-й Исследовательской комиссии 4](#_Toc95234803)

[1.2 Руководящий состав и собрания, проведенные 17-й Исследовательской комиссией 5](#_Toc95234804)

[2 Организация работы 11](#_Toc95234805)

[2.1 Организация исследований и распределение работы 11](#_Toc95234806)

[2.2 Вопросы и Докладчики 14](#_Toc95234807)

[3 Результаты работы, завершенной в течение исследовательского периода 2017−2020 годов 20](#_Toc95234808)

[3.1 Общая информация 20](#_Toc95234809)

[3.2 Важнейшие результаты деятельности 20](#_Toc95234810)

[а) Вопрос 1/17 − Координация деятельности в области безопасности электросвязи/ИКТ (2017−2020 гг.)/Стратегия и координация стандартизации в области безопасности (2021 г. −) 21](#_Toc95234811)

[b) Вопрос 2/17 − Архитектура и структура безопасности (2017−2020 гг.)/  
Архитектура безопасности и безопасность сетей (2021 г. −) 21](#_Toc95234812)

[c) Вопрос 3/17 − Управление безопасностью информации, передаваемой   
по системам электросвязи (2017−2020 гг.)/Управление безопасностью   
информации, передаваемой с помощью электросвязи, и услуги по   
обеспечению безопасности (2021 г. −) 23](#_Toc95234813)

[d) Вопрос 4/17 − Кибербезопасность (2017−2020 гг.)/Кибербезопасность и   
противодействие спаму (2021 г. −) 24](#_Toc95234814)

[e) Вопрос 5/17 − Противодействие распространению спама техническими   
средствами (2017−2020 гг.) 27](#_Toc95234815)

[f) Вопрос 6/17 − Аспекты безопасности услуг и сетей электросвязи,   
а также интернета вещей (2017−2020 гг.)/Безопасность услуг электросвязи и интернета вещей (2021 г. −) 28](#_Toc95234816)

[g) Вопрос 7/17 − Безопасные прикладные услуги 30](#_Toc95234817)

[h) Вопрос 8/17 − Безопасность облачных вычислений и инфраструктуры   
больших данных 31](#_Toc95234818)

[i) Вопрос 9/17 − Телебиометрия (2017−2020 гг.) 32](#_Toc95234819)

[j) Вопрос 10/17 − Архитектура и механизмы управления определением   
идентичности (2017−2020 гг.)/Архитектура и механизмы управления   
определением идентичности и телебиометрии (2021 г. −) 33](#_Toc95234820)

[k) Вопрос 11/17 − Общие технологии (Справочник, инфраструктура   
открытых ключей (PKI), инфраструктура управления привилегиями (PMI), абстрактная синтаксическая нотация № 1 (ASN.1), идентификаторы объектов (OID)) для поддержки безопасных приложений (2017−2020 гг.)/Общие   
технологии (например, Справочник, PKI, формальные языки, идентификаторы объекта) для поддержки безопасных приложений (2021 г. −) 35](#_Toc95234821)

[l) Вопрос 12/17 − Формальные языки для программного обеспечения систем   
электросвязи и тестирования (2017−2020 гг.) 40](#_Toc95234822)

[m) Вопрос 13/17 − Аспекты безопасности для интеллектуальной транспортной   
системы 2017−2020 гг.)/ Безопасность интеллектуальных транспортных   
систем (ИТС) (2021 г. −) 44](#_Toc95234823)

[n) Вопрос 14/17 − Аспекты безопасности технологии распределенного реестра (2018−2020 гг.)/Безопасность технологии распределенного реестра (DLT)   
(2021 г. −) 45](#_Toc95234824)

[o) Вопрос 15/17 – Безопасность для/с помощью появляющихся технологий,   
включая квантовую безопасность 47](#_Toc95234825)

[3.3 Отчет о деятельности ведущей исследовательской комиссии, ГИС, JCA,   
региональных групп и проектов 47](#_Toc95234826)

[3.3.1 Деятельность ведущей исследовательской комиссии по вопросам   
безопасности 47](#_Toc95234827)

[3.3.2 Деятельность ведущей исследовательской комиссии по вопросам   
управления определением идентичности 51](#_Toc95234828)

[3.3.3 Деятельность ведущей исследовательской комиссии по вопросам   
языков и методов описания 52](#_Toc95234829)

[3.3.4 Совместная координационная деятельность по управлению определением идентичности (JCA-IdM) 53](#_Toc95234830)

[3.3.5 Региональная группа 17-й Исследовательской комиссии для Африки   
(РегГр-АФР ИК17) 53](#_Toc95234831)

[3.3.6 Региональная группа ИК17 МСЭ для Арабского региона   
(РегГр-АРБ ИК17) 54](#_Toc95234832)

[3.4 Проекты 54](#_Toc95234833)

[3.4.1 Проект ASN.1 54](#_Toc95234834)

[3.4.2 Проект OID 54](#_Toc95234835)

[3.5 Преодоление разрыва в стандартизации 55](#_Toc95234836)

[4 Замечания, касающиеся будущей работы 55](#_Toc95234837)

[5 Обновления к Резолюции 2 ВАСЭ на исследовательский период 2022−2024 годов 57](#_Toc95234838)

[ПРИЛОЖЕНИЕ 1](#_Toc95234839) – [Список Рекомендаций, Добавлений и других материалов, разработанных   
или исключенных в течение исследовательского периода 58](#_Toc95234840)

[ПРИЛОЖЕНИЕ 2](#_Toc95234841) – [Предлагаемый пересмотр к Резолюции 2 ВАСЭ 74](#_Toc95234842)

# 1 Введение

## 1.1 Сфера ответственности 17-й Исследовательской комиссии

Всемирная ассамблея по стандартизации электросвязи (Хаммамет, 2016 г.) поручила 17‑й Исследовательской комиссии исследование 12 Вопросов, направленных на укрепление доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ).

В Приложении A к Резолюции 2 ВАСЭ-16 установлен следующий мандат 17-й Исследовательской комиссии (Безопасность):

*17-я Исследовательская комиссия МСЭ-Т отвечает за формирование доверия и обеспечение безопасности при использовании информационно‑коммуникационных технологий (ИКТ). Сюда относится проведение исследований, относящихся к вопросам кибербезопасности, управления безопасностью, противодействия спаму и управления определением идентичности. Сюда относятся также вопросы архитектуры и структуры безопасности, защиты информации, позволяющей установить личность, а также безопасности приложений и услуг для интернета вещей (IoT), "умных" электросетей, смартфонов, организации сетей с программируемыми параметрами (SDN), телевидения на основе протокола Интернет (IPTV), веб‑услуг, социальных сетей, облачных вычислений, анализа больших данных, мобильной финансовой системы и телебиометрии. 17‑я Исследовательская комиссия также отвечает за приложения открытых систем связи, в том числе каталоги и идентификаторы объектов, за технические языки, метод их использования и другие вопросы, относящиеся к аспектам программного обеспечения систем электросвязи, и за языки спецификации тестирования для поддержки проверки на соответствие в целях повышения качества Рекомендаций.*

В Приложении A к Резолюции 2 ВАСЭ-16 определены следующие сферы ответственности 17‑й Исследовательской комиссии (Безопасность) в качестве ведущей исследовательской комиссии:

*− ведущая исследовательская комиссия по вопросам безопасности;*

*− ведущая исследовательская комиссия по вопросам управления определением идентичности (IdM);*

*− ведущая исследовательская комиссия по вопросам языков и методов описания.*

В Приложении B к Резолюции 2 ВАСЭ-16 для ИК17 установлены следующие руководящие ориентиры:

*17-я Исследовательская комиссия МСЭ-Т отвечает за формирование доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ). Сюда относится проведение исследований, касающихся безопасности, в том числе кибербезопасности, противодействия спаму и управления определением идентичности. Сюда относятся также вопросы архитектуры и структуры безопасности, управления обеспечением безопасности, защиты информации, позволяющей установить личность (PII), а также безопасности приложений и услуг для интернета вещей (IoT), "умных" электросетей, смартфонов, организации сетей с программируемыми параметрами (SDN), телевидения на основе протокола Интернет (IPTV), веб-услуг, социальных сетей, облачных вычислений, мобильной финансовой системы и телебиометрии. 17‑я Исследовательская комиссия также отвечает за вопросы применения открытых систем связи, включая каталог и идентификаторы объектов, за технические языки, методы их использования и другие вопросы, связанные с аспектами систем электросвязи, касающимися программного обеспечения, а также за проверку на соответствие в целях повышения качества Рекомендаций.*

*В области безопасности 17-я Исследовательская комиссия отвечает за разработку основных Рекомендаций по таким вопросам безопасности ИКТ, как архитектура и структуры безопасности; основы, касающиеся кибербезопасности, включая угрозы, уязвимости и риски, реагирование/реакция на инциденты и цифровую техническую экспертизу; управление безопасностью, включая управление PII; а также борьба со спамом техническими средствами. Кроме того, 17‑я Исследовательская комиссия обеспечивает общую координацию деятельности в области безопасности в рамках МСЭ‑Т.*

*Помимо этого, 17-я Исследовательская комиссия отвечает за разработку основных Рекомендаций по аспектам безопасности приложений и услуг в области IPTV, "умных" электросетей, IoT, организации сетей с программируемыми параметрами (SDN), социальных сетей, облачных вычислений, анализа больших данных, смартфонов, мобильной финансовой системы и телебиометрии.*

*17-я Исследовательская комиссия отвечает также за разработку основных Рекомендаций по общей модели управления идентичностью, которая не зависит от сетевых технологий и поддерживает безопасный обмен информацией об идентичности между объектами. Эта работа также включает в себя исследование процесса обнаружения авторитетных источников информации об идентичности; общие механизмы для соединения/ функционального взаимодействия различных наборов форматов информации об идентичности; угроз управлению определением идентичности, механизмов противодействия им, защиту информации, позволяющей установить личность (PII), и разработку механизмов обеспечения того, чтобы доступ к PII был разрешен только в случае необходимости.*

*В том что касается открытых систем связи, 17-я Исследовательская комиссия отвечает за Рекомендации в следующих областях:*

*• справочные службы и системы, включая инфраструктуру открытых ключей (PKI) (серии МСЭ‑Т F.500 и МСЭ-Т Х.500);*

*• идентификаторы объектов (OID) и связанные с ними органы регистрации (серии МСЭ‑Т X.660/МСЭ-Т X.670);*

*• взаимосвязь открытых систем (OSI), включая абстрактную синтаксическую нотацию версии 1 (ASN.1) (серии МСЭ-Т F.400, МСЭ-Т X.200, МСЭ-Т X.400, МСЭ‑Т X.600, МСЭ‑Т X.800); и*

*• открытая распределенная обработка (ODP) (серии МСЭ-Т Х.900).*

*В области языков 17-я Исследовательская комиссия отвечает за проведение исследований, касающихся методов моделирования, спецификации и описания, которые включают такие языки, как ASN.1, SDL, MSC, URN и TTCN-3.*

*Эта работа будет проводиться в соответствии с потребностями соответствующих исследовательских комиссий, таких как 2-я, 9-я, 11-я, 13-я, 15-я, 16-я и 20‑я исследовательские комиссии (по вопросам безопасности IoT и SC&C), и в сотрудничестве с ними.*

*17-я Исследовательская комиссия будет работать над соответствующими аспектами управления определением идентичности в сотрудничестве с 20-й Исследовательской комиссией по вопросам IoT и с 2-й Исследовательской комиссией согласно мандату каждой исследовательской комиссии.*

В Приложении C к Резолюции 2 ВАСЭ-16 (с внесенными КГСЭ изменениями) приведен перечень Рекомендаций, входящих в сферу ответственности 17-й Исследовательской комиссии в течение исследовательского периода 2017−2020 гг.:

*− МСЭ-Т E.104, МСЭ-Т E.115, МСЭ-Т E.409 (совместно с 2-й Исследовательской комиссией);*

*− серия МСЭ-Т F.400; МСЭ-Т F.500 – МСЭ-Т F.549;*

*− серия МСЭ-Т Х, за исключением тех Рекомендаций, которые входят в сферу ответственности 2‑й, 11-й, 13-й, 15-й и 16‑й Исследовательских комиссий;*

*− серия МСЭ-Т Z, за исключением серии МСЭ-Т Z.300 и серии МСЭ-Т Z.500.*

## 1.2 Руководящий состав и собрания, проведенные 17-й Исследовательской комиссией

На ВАСЭ-16 был назначен председатель 17‑й Исследовательской комиссии – г-н ЮМ Хён-Юл (Республика Корея) и следующие девять заместителей председателя 17‑й Исследовательской комиссии: г-н ДОЛМАТОВ Василий (Российская Федерация), г-н ИШАГ Муатаз Эльсадиг (Судан), г-н ЭВРЕН Гохан (Турция), г-жа ФУРЕЙ Инетт (Соединенные Штаты Америки), г-жа ЛАТРУС Уала Тюрки (Тунис), г-н ЛИНЬ Чжаоцзи (Китай), г-н МИГЕЛЬ Уго Дарио (Аргентина), г-н МИЯКЕ Ютака (Япония) и г-н КЕТТИН-ЗАНГА Патрик-Кеннеди (Центральноафриканская Республика). Г-н КЕТТИН-ЗАНГА Патрик-Кеннеди не принял участия ни в одном собрании 17‑й Исследовательской комиссии в этом исследовательском периоде.

В марте 2018 года г-н ГОНCАЛЕС Хуан (Соединенные Штаты Америки) заменил на посту заместителя председателя 17-й Исследовательской комиссии г-жу ФУРЕЙ Инетт (Соединенные Штаты Америки). В марте 2020 года г-жа МОЛИНАРИ Лиа (Аргентина) заменила на посту заместителя председателя 17-й Исследовательской комиссии г-на МИГЕЛЯ Уго Дарио (Аргентина). В августе 2020 года г-н МБАТАС Эрик Анисет (Центральноафриканская Республика) заменил на посту заместителя председателя 17-й Исследовательской комиссии г-на КЕТТИНА-ЗАНГУ Патрика-Кеннеди (Центральноафриканская Республика).

17-я Исследовательская комиссия в течение рассматриваемого исследовательского периода провела десять пленарных заседаний (см. Таблицу 1).

ТАБЛИЦА 1

Собрания 17-й Исследовательской комиссии и ее рабочих групп

| Собрания | Дата | Отчеты |
| --- | --- | --- |
| 17-я Исследовательская комиссия/ ее рабочие группы | Женева, 22−30 марта 2017 г. | SG17 − R1 − R9 |
| 17-я Исследовательская комиссия/ ее рабочие группы | Женева, 29 августа − 6 сентября 2017 г. | SG17 − R10 − R17 |
| 17-я Исследовательская комиссия/ ее рабочие группы | Женева, 20−29 марта 2018 г. | SG17 − R18 − R24 |
| 17-я Исследовательская комиссия/ ее рабочие группы | Женева, 29 августа − 7 сентября 2018 г. | SG17 − R25 − R32 |
| 17-я Исследовательская комиссия/ ее рабочие группы | Женева, 22−30 января 2019 г. | SG17 − R33 − R37 |
| 17-я Исследовательская комиссия/ ее рабочие группы | Женева, 27 августа − 5 сентября 2019 г. | SG17 − R38 − R50 |
| 17-я Исследовательская комиссия/ ее рабочие группы | Виртуальное, 17−26 марта 2020 г. | SG17 − R51 − R66 |
| 17-я Исследовательская комиссия | Виртуальное, 29 мая 2020 г. | SG17 − R67 |
| 17-я Исследовательская комиссия/ ее рабочие группы | Виртуальное, 24 августа − 3 сентября 2020 г. | SG17 − R68 − R77 |
| 17-я Исследовательская комиссия | Виртуальное, 7 января 2021 г. | SG17 − R78 |
| 17-я Исследовательская комиссия/ ее рабочие группы | Виртуальное, 20−30 апреля 2021 г. | SG17 − R79 − R85 |
| 17-я Исследовательская комиссия/ ее рабочие группы | Виртуальное, 24 августа – 3 сентября 2020 г. | SG17 − R86 − R102 |
| 17-я Исследовательская комиссия | Виртуальное, 7 января 2022 г. | SG17 − R103 |

Открытое расширенное собрание руководящего состава проводилось в сочетании с каждым собранием 17-й Исследовательской комиссии.

Наряду с этим в различных местах в течение исследовательского периода прошли многочисленные собрания групп Докладчиков, см. Таблицу 1*bis*.

ТАБЛИЦА 1*bis*

Собрания групп Докладчиков, организованные под руководством 17-й Исследовательской комиссии   
в течение исследовательского периода

| Даты | Место проведения/ принимающая сторона | Вопрос(ы) | Название мероприятия |
| --- | --- | --- | --- |
| 12.12.2016 г. − 13.12.2016 г. | Китай [Пекин] | [8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5710&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0057)] | Собрание Группы Докладчика по Вопросу 8/17 в промежуточный период |
| 12.01.2017 г. − 13.01.2017 г. | *Электронное собрание* | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5711&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0054)] | Электронное собрание Группы Докладчика по Вопросу 4/17 в промежуточный период |
| 06.02.2017 г. − 10.02.2017 г. | Тунис [Тунис] | [11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5716&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0058)] | Совместное собрание Группы Докладчика по Вопросу 11/17 с РГ10 ПК6 ОТК1 ИСО/МЭК |
| 08.02.2017 г. − 09.02.2017 г. | Корея (Республика) [Сеул] | [3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5712&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0053)] | Собрание Группы Докладчика по Вопросу 3/17 в промежуточный период |
| 08.02.2017 г. − 09.02.2017 г. | Корея (Республика) [Сеул] | [6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5713&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0056)] | Собрание Группы Докладчика по Вопросу 6/17 в промежуточный период |
| 22.06.2017 г. − 23.06.2017 г. | Корея (Республика) [Сеул] | [3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6903&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0392)] | Промежуточное собрание Группы Докладчика по Вопросу 3/17 |
| 22.06.2017 г. − 23.06.2017 г. | Корея (Республика) [Сеул] | [6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6904&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0393)] | Промежуточное собрание Группы Докладчика по Вопросу 6/17 |
| 27.06.2017 г. − 28.06.2017 г. | Китай [Пекин] | [8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6909&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0394)] | Промежуточное собрание Группы Докладчика по Вопросу 8/17 |
| 29.06.2017 г. | Япония [Токио] | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6916&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0395)] | Промежуточное собрание Группы Докладчика по Вопросу 4/17 |
| 30.06.2017 г | Япония [Токио] | [3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6905&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)] [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6906&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)] [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6907&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)] | Совместное собрание Групп Докладчиков по Вопросам 3/17, 4/17 и 10/17, посвященное ЦФУ |
| 03.07.2017 г. | Япония [Токио] | [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=7916&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0396)] | Промежуточное собрание Группы Докладчика по Вопросу 10/17 |
| 14.07.2017 г. | Корея (Республика) [Сеул] | [13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=8918&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0397)] | Промежуточное собрание Группы Докладчика по Вопросу 13/17 |
| 30.10.2017 г. −  03.11.2017 г. | Корея (Республика) | [11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9047&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817)] | Совместное собрание Группы Докладчика по Вопросу 11/17 с ПК6 ОТК1 ИСО/МЭК |
| 30.11.2017 г. −  01.12.2017 г. | Корея (Республика) [Bundang] | [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9048&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817)] | Собрание Группы Докладчика по Вопросу 14/17 |
| 13.12.2017 г. −  14.12.2017 г. | Китай [Пекин] | [7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9050&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0822)] | Собрание Группы Докладчика по Вопросу 7/17 |
| 09.01.2018 г. | Канада [Ванкувер] | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9051&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0821)] [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9052&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-1006)] | Совместное собрание Групп Докладчиков по Вопросам 4/17 и 10/17 |
| 22.01.2018 г. −  23.01.2018 г. | Китай [Пекин] | [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9057&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0823)] | Собрание Группы Докладчика по Вопросу 14/17 |
| 24.01.2018 г. −  25.01.2018 г. | Корея (Республика) [Сеул] | [13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9056&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0818)] | Собрание Группы Докладчика по Вопросу 13/17 |
| 25.01.2018 г. −  26.01.2018 г. | Корея (Республика) [Сеул] | [3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9054&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0820)] | Собрание Группы Докладчика по Вопросу 3/17 |
| 25.01.2018 г. −  26.01.2018 г. | Корея (Республика) [Сеул] | [6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9055&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0819)] | Собрание Группы Докладчика по Вопросу 6/17 |
| 04.06.2018 г. −  06.06.2018 г. | Китай [Пекин] | [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9265&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1252)] | Промежуточное собрание Группы Докладчика по Вопросу 14/17 |
| 07.06.2018 г. −  08.06.2018 г. | Корея (Республика) [Сеул] | [6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9261&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1246)] [13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9262&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1251)] | Промежуточное собрание Группы Докладчика по Вопросам 6/17 и 13/17 |
| 20.06.2018 г. −  21.06.2018 г. | Китай [Yinchuan] | [7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9259&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1247)] | Собрание Группы Докладчика по Вопросу 7/17 |
| 26.06.2018 г. −  27.06.2018 г. | Соединенные Штаты Америки [Сиэтл, Вашингтон] | [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9264&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1249)] | Промежуточное собрание Группы Докладчика по Вопросу 10/17 |
| 27.06.2018 г. −  28.06.2018 г. | Китай [Пекин] | [8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9263&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1248)] | Промежуточное собрание Группы Докладчика по Вопросу 8/17 |
| 27.08.2018 г. −  31.08.2018 г. | Япония [Токио] | [11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9260&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1250)] | Промежуточное собрание Группы Докладчика по Вопросу 11/17 совместно с РГ10 ПК6 ОТК1 ИСО/МЭК |
| 08.11.2018 г. −  09.11.2018 г. | Сингапур | [13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9405&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1727)] | Промежуточные собрания Группы Докладчика по Вопросу 13/17 |
| 12.11.2018 г. −  13.11.2018 г. | Япония [Токио] | [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9406&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726)] | Промежуточные собрания Группы Докладчика по Вопросу 10/17 |
| 12.11.2018 г. −  13.11.2018 г. | Япония [Токио] | [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9407&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726)] | Промежуточные собрания Группы Докладчика по Вопросу 14/17 |
| 22.04.2019 г. −  26.04.2019 г. | Китай [Пекин] | [11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9560&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2057)] | Промежуточное собрание Группы Докладчика по Вопросу 11/17 в сотрудничестве с РГ10 ПК6 ОТК1 ИСО/МЭК |
| 04.06.2019 г. −  05.06.2019 г. | *Электронное собрание* | [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9559&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2056)] | Промежуточное электронное собрание Группы Докладчика по Вопросу 10/17 |
| 04.06.2019 г. −  05.06.2019 г. | *Электронное собрание* | [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9563&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2059)] | Промежуточное собрание Группы Докладчика по Вопросу 14/17 |
| 10.06.2019 г. −  12.06.2019 г. | Китай [Шанхай] | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9574&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2051)] | Промежуточное собрание Группы Докладчика по Вопросу 4/17 |
| 11.06.2019 г. −  12.06.2019 г. | Китай [Пекин] | [13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9561&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2058)] | Промежуточное собрание Группы Докладчика по Вопросу 13/17 |
| 18.06.2019 г. −  19.06.2019 г. | Китай [Чунцин] | [7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9556&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2053)] | Промежуточное собрание Группы Докладчика по Вопросу 7/17 |
| 24.06.2019 г. −  25.06.2019 г. | Китай [Пекин] | [8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9557&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2054)] | Промежуточное собрание Группы Докладчика по Вопросу 8/17 |
| 27.06.2019 г. −  28.06.2019 г. | Япония [Токио] | [6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9555&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2052)] | Промежуточное собрание Группы Докладчика по Вопросу 6/17 |
| 27.06.2019 г. | *Электронное собрание* | [3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9554&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2050)] | Промежуточное электронное собрание Группы Докладчика по Вопросу 3/17 |
| 22.10.2019 г. −  23.10.2019 г. | Китай | [7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9763&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2564)] | Промежуточное собрание Группы Докладчика по Вопросу 7/17 |
| 05.12.2019 г. −  06.12.2019 г. | Швейцария [Фрибург] | [11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9767&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762)]  [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9768&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762)] | Совместное собрание Групп Докладчиков по Вопросам 11/17 и 14/17 |
| 11.12.2019 г. −  13.12.2019 г. | Китай [Цзинань] | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9882&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2562)] | Промежуточное собрание Группы Докладчика по Вопросу 4/17 |
| 11.12.2019 г. | *Электронное собрание* | [11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9766&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2567)] | Промежуточное собрание Группы Докладчика по Вопросу 11/17 |
| 11.12.2019 г. | Китай [Цзинань] | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9760&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2754)] | Приближенные по срокам собрания Групп Докладчиков по Вопросам 4/17 и 16/13 |
| 12.12.2019 г. | Япония [Токио] | [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9765&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2566)] | Промежуточное собрание Группы Докладчика по Вопросу 10/17 |
| 13.12.2019 г. | Япония [Токио] | [3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9759&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2561)] | Промежуточное собрание Группы Докладчика по Вопросу 3/17 |
| 07.01.2020 г. − 08.01.2020 г. | Китай [Пекин] | [8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9764&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2565)] | Промежуточное собрание Группы Докладчика по Вопросу 8/17 |
| 07.01.2020 г.−  08.01.2020 г. | Япония [Фукуока] | [13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9769&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2569)] | Промежуточное собрание Группы Докладчика по Вопросу 13/17 |
| 08.01.2020 г. | *Электронное собрание* | [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9771&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2570)] | Промежуточное собрание Группы Докладчика по Вопросу 14/17 |
| 13.01.2020 г. − 14.01.2020 г. | Малайзия [Куала-Лумпур] | [6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9783&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2563)] | Промежуточное собрание Группы Докладчика по Вопросу 6/17 |
| 03.02.2020 г. − 07.02.2020 г. | Соединенное Королевство [Лондон] | [11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9770&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2568)] | Промежуточное собрание Группы Докладчика по Вопросу 11/17 в сотрудничестве с РГ10 ПК6 ОТК1 ИСО/МЭК |
| 17.04.2020 г. | *Электронное собрание* | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10081&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2963)] | Промежуточное собрание Группы Докладчика по Вопросу 4/17 |
| 22.04.2020 г. | *Электронное собрание* | [11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10087&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2966)] | Промежуточное собрание Группы Докладчика по Вопросу 11/17 |
| 11.05.2020 г.−  12.05.2020 г. | *Электронное собрание* | [6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10083&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3093)] | Промежуточное собрание Группы Докладчика по Вопросу 6/17 |
| 13.05.2020 г. | *Электронное собрание* | [13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10088&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2979)] | 13/17 Промежуточное собрание Группы Докладчика по Вопросу |
| 02.06.2020 г. −  03.06.2020 г. | *Электронное собрание* | [3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10080&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3090)] | Промежуточное собрание Группы Докладчика по Вопросу 3/17 |
| 10.06.2020 г. −  11.06.2020 г. | *Электронное собрание* | [13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10089&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3096)] | Промежуточное собрание Группы Докладчика по Вопросу 13/17 |
| 19.06.2020 г. | *Электронное собрание* | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10347&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3091)] | Промежуточное собрание Группы Докладчика по Вопросу 4/17 |
| 22.06.2020 г. −  23.06.2020 г. | *Электронное собрание* | [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10090&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3097)] | Промежуточное собрание Группы Докладчика по Вопросу 14/17 |
| 13.07.2020 г. | *Электронное собрание* | [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10086&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3095)] | Промежуточное собрание Группы Докладчика по Вопросу 10/17 |
| 16.07.2020 г. −  17.07.2020 г. | *Электронное собрание* | [8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10084&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3094)] | Промежуточное собрание Группы Докладчика по Вопросу 8/17 |
| 19.10.2020 г. −  30.10.2020 г. | *Электронное собрание* | [11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11694&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3447)] | Промежуточное собрание Группы Докладчика по Вопросу 11/17 в сотрудничестве с РГ10 ПК6 ОТК1 ИСО/МЭК |
| 18.11.2020 г. | *Электронное собрание* | [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11588&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3462)] | Промежуточное собрание Группы Докладчика по Вопросу 10/17 |
| 25.11.2020 г. − 26.11.2020 г. | *Электронное собрание* | [13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11589&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3467)] | Промежуточное собрание Группы Докладчика по Вопросу 13/17 |
| 26.11.2020 г. − 27.11.2020 г. | *Электронное собрание* | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11570&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3460)] | Промежуточное собрание Группы Докладчика по Вопросу 4/17 |
| 07.12.2020 г. − 08.12.2020 г. | *Электронное собрание* | [2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11569&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3459)] | Промежуточное собрание Группы Докладчика по Вопросу 2/17 |
| 09.12.2020 г. − 10.12.2020 г. | *Электронное собрание* | [3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11727&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3468)] | Промежуточное собрание Группы Докладчика по Вопросу 3/17 |
| 21.12.2020 г. − 22.12.2020 г. | *Электронное собрание* | [6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11571&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3463)] | Промежуточное собрание Группы Докладчика по Вопросу 6/17 |
| 04.01.2021 г. − 05.01.2021 г. | *Электронное собрание* | [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11590&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3469)] | Промежуточное собрание Группы Докладчика по Вопросу 14/17 |
| 01.02.2021 г. − 02.02.2021 г. | *Электронное собрание* | [3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11832&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3547)] | Промежуточное собрание Группы Докладчика по Вопросу 3/17 |
| 01.02.2021 г. − 02.02.2021 г. | *Электронное собрание* | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11830&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3548)] | Промежуточное собрание Группы Докладчика по Вопросу 4/17 |
| 04.02.2021 г. | *Электронное собрание* | [6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11571&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3463)] | Промежуточное собрание Группы Докладчика по Вопросу 6/17 |
| 17.06.2021 г. −  18.06.2021 г. | *Электронное собрание* | [15/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12574&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3876)] | Промежуточное собрание Группы Докладчика по Вопросу 15/17 |
| 17.06.2021 г. −  18.06.2021 г. | *Электронное собрание* | [8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12539&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3875)] | Промежуточное собрание Группы Докладчика по Вопросу 8/17 |
| 24.06.2021 г. −  25.06.2021 г. | *Электронное собрание* | [4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12534&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3877)] | Промежуточное собрание Группы Докладчика по Вопросу 4/17 |
| 24.06.2021 г. | *Электронное собрание* | [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12575&Group=17) [[отчет о собрании](http://www.itu.int/md/T17-SG17-210824-TD-PLEN-3878)] | Промежуточное собрание Группы Докладчика по Вопросу 10/17 |
| 28.06.2021 г. −  29.06.2021 г. | *Электронное собрание* | [14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12592&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3879)] | Промежуточное собрание Группы Докладчика по Вопросу 14/17 |
| 01.07.2021 г. −  02.07.2021 г. | *Электронное собрание* | [2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12533&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3880)] | Промежуточное собрание Группы Докладчика по Вопросу 2/17 |
| 05.10.2021 г | *Электронное собрание* | [3/17 [отчет о собрании]](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4199/en) | Промежуточное собрание Группы Докладчика по Вопросу 3/17 |
| 19.11.2021 г. | *Электронное собрание* | [10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12744&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4178)] | Промежуточное собрание Группы Докладчика по Вопросу 10/17 |
| 24.11.2021 г. −  25.11.2021 г. | *Электронное собрание* | [2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12733&Group=17) [[отчет о собрании](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4159)] | Промежуточное собрание Группы Докладчика по Вопросу 2/17 |
| 20.01.2022 г. −  21.01.2022- г. | *Электронное собрание* | 15/17 [отчет о собрании] | Промежуточное собрание Группы Докладчика по Вопросу 15/17 |
| 07.02.2022 г. | *Электронное собрание* | 3/17 [отчет о собрании] | Промежуточное собрание Группы Докладчика по Вопросу 3/17 |
| 15.02.2022 г. | *Электронное собрание* | 10/17 [отчет о собрании] | Промежуточное собрание Группы Докладчика по Вопросу 10/17 |
| 17.02.2022 г. | *Электронное собрание* | 6/17 [отчет о собрании] | Промежуточное собрание Группы Докладчика по Вопросу 6/17 |
| 23.02.2022 г. −  24.02.2022 г. | *Электронное собрание* | 2/17 [отчет о собрании] | Промежуточное собрание Группы Докладчика по Вопросу 2/17 |
| ??.02.2022 г. | *Электронное собрание* | 4/17 [отчет о собрании] | Промежуточное собрание Группы Докладчика по Вопросу 4/17 |

# 2 Организация работы

## 2.1 Организация исследований и распределение работы

**2.1.1** На своем первом собрании в исследовательском периоде 17-я Исследовательская комиссия приняла решение создать четыре рабочих группы. В Таблице 2 представлены номер и название каждой рабочей группы, порученные ей Вопросы, а также фамилии ее председателя и заместителей председателя в период с 2017 по 2020 год.

ТАБЛИЦА 2

Организация 17-й Исследовательской комиссии (2017−2020 гг.)

| Название | Вопросы для исследования | Название  Рабочей группы | Председатель  и заместители председателя |
| --- | --- | --- | --- |
| PLEN | 1/17 |  |  |
| РГ 1/17 | 2/17; 3/17; 6/17; 13/17 (7) | Безопасность электросвязи/ИКТ | г-н Мияке Ютака (Председатель) г-н Долматов Василий (заместитель председателя) г-н Эврен Гохан (заместитель председателя) |
| РГ 2/17 | 4/17; 5/17; 14/17 (8) | Безопасность киберпространства | г-н Накао Koдзи (Председатель) г-жа Фурей Инетт (заместитель председателя) (1)г-н Гонсалес Хуан (заместитель председателя)(2) |
| РГ 3/17 | 7/17; 8/17; 12/17 | Безопасность приложений | г-н Таддей Арно (Председатель) г-н Линь Чжаоцзи (заместитель председателя) (3)г-жа Бай Сяоюань (заместитель председателя) (4) |
| РГ 4/17 | 9/17; 10/17; 11/17 | Управление идентичностью и аутентификация | г-н Ли Кэпэн (Председатель)(5)г-н Хун Джэ На (заместитель председателя/ Сопредседатель)(5, 6) г-н Линь Чжаоцзи (Сопредседатель) (6) |
| Примечания:  (1) Заместитель председателя до сентября 2017 года.  (2) Заместитель председателя с марта 2018 года.  (3) Заместитель председателя до сентября 2018 года.  (4) Заместитель председателя с января 2019 года.  (5) Председатель/Заместитель председателя до сентября 2018 года.  (6) Сопредседатель с января 2019 года.  (7) Группа Докладчика по Вопросу 13/17 учреждена ИК17 в сентябре 2017 года.  (8) Группа Докладчика по Вопросу 14/17 учреждена ИК17 в марте 2018 года. | | | |

**2.1.2** В связи со вспышкой глобальной пандемии COVID-19 проведение Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ-20), запланированное на 2020 год, было перенесено на 2022 год, а исследовательский период 2017–2020 годов соответственно продлен до ВАСЭ-20. В августе/  
сентябре 2020 года собрание ИК17 согласовало комплекс из 12 Вопросов для утверждения ВАСЭ-20 (см. раздел 2.2) и создание целевой группы по подготовке к следующему исследовательскому периоду.

В связи с переносом ВАСЭ-20 на март 2022 года собрание КГСЭ, состоявшееся 11−18 января 2021 года, одобрило этот новый комплекс Вопросов ИК17 (см. [Циркуляр 295 БСЭ](https://www.itu.int/md/T17-TSB-CIR-0295/en)). На собрании, состоявшемся 20–30 апреля 2021 года, ИК17 приняла решение организовать новую структуру комплекса из 12 Вопросов, состоящую из пяти рабочих групп.

В Таблице 3 представлены номер и название каждой рабочей группы, порученные ей Вопросы, а также фамилия ее председателя начиная с 2021 года

ТАБЛИЦА 3

Организация 17-й Исследовательской комиссии (2021 г. −)

| Название | Вопросы для исследования | Название  Рабочей группы | Председатель  и заместители председателя |
| --- | --- | --- | --- |
| РГ 1/17 | 1/17; 15/17 | Стратегия и координация стандартизации в области безопасности | Председатель:  г-н Долматов Василий (Россия)  заместитель председателя:  г-н Ким Чон Юн (Корея) |
| РГ 2/17 | 2/17; 6/17; 13/17 | Безопасность 5G, IoT и ИТС | Председатель:  г-н Мияке Ютака (KDDI)  Заместители председателя:  г-жа Ху Чжиюань (Nokia Shanghai Bell)  г-н Миллс Филип (Соединенное Королевство) |
| РГ 3/17 | 3/17; 4/17 | Кибербезопасность и управление | Председатель:  г-н Накао Koдзи (NICT)  Заместитель председателя:  г-жа Молинари Лиа (Аргентина) |
| РГ 4/17 | 7/17; 8/17; 14/17 | Безопасность услуг и приложений | Председатель:  г-н На Джэ Хун (ETRI)  Заместитель председателя:  г-жа Бай Сяоюань (Alibaba) |
| РГ 5/17 | 10/17; 11/17 | Основные технологии безопасности | Председатель:  г-н Линь Чжаоцзи (ZTE)  Заместитель председателя:  *вакантный пост* |

**2.1.3** В Таблице 4 перечислены другие группы, созданные 17-й Исследовательской комиссией в течение исследовательского периода.

**2.1.4** В соответствии с Резолюцией 54 ВАСЭ-16 на своем собрании в марте 2017 года ИК17 создала Региональную группу ИК17 для Арабского региона, см. раздел 3.3.5.

**2.1.5** В течение рассматриваемого исследовательского периода была продолжена и одобрена КГСЭ работа двух **групп по совместной координационной деятельности (JCA)**, предложенных 17‑й Исследовательской комиссией.

– **Группа по совместной координационной деятельности по управлению определением идентичности (JCA-IdM)**

Работа Группы по совместной координационной деятельности по управлению определением идентичности (JCA-IdM) продолжалась после предшествующего исследовательского периода, и ее задача заключалась в координации деятельности МСЭ-T в области управления определением идентичности (IdM) в сотрудничестве с внешними органами. Основная информация о результатах работы Группы JCA-IdM приведена в пункте 3.3.4.

– **Группа по совместной координационной деятельности по защите ребенка в онлайновой среде (JCA-COP)**

Работа Группы по совместной координационной деятельности по защите ребенка в онлайновой среде(JCA-COP), продолжавшаяся после предшествующего исследовательского периода, была приостановлена на первом собрании ИК17, состоявшемся в марте 2017 года.

**2.1.6** В течение рассматриваемого исследовательского периода 17-й Исследовательская комиссия продолжала выполнять два **проекта**.

– **Проект ASN.1**

В рамках проекта ASN.1, учрежденного в течение исследовательского периода 2001−2004 годов, продолжается оказание помощи пользователям ASN.1 (Рекомендации МСЭ-Т серий X.680, X.690 и X.890), как в МСЭ-Т, так и за его пределами, и содействие использованию ASN.1 в широком диапазоне различных отраслей и органов по стандартизации. Основная информация о результатах выполнения данного проекта приведена в пункте 3.4.1.

– **Проект OID**

В рамках проекта OID, учрежденного в течение исследовательского периода 2001−2004 годов, продолжается оказание помощи и содействия пользователям идентификаторов объектов (OID), зарегистрированных в соответствии с Рекомендациями серий X.660 и X.670, как в МСЭ-Т, так и за его пределами. Основная информация о результатах выполнения данного проекта приведена в пункте 3.4.2.

ТАБЛИЦА 4

Другие группы (если таковые имеются)

|  |  |  |
| --- | --- | --- |
| Название группы | Председатель | Заместители председателя |
| JCA-IdM | Сопредседатели:  г-н Эбби Барбир (1) г-н Кындуг Парк (1) г-н Хироси Такети (1) г-н ЮМ Хён-Юл (8) |  |
| JCA-COP | Неприменимо |  |
| РегГр-АФР ИК17 | г-н Майкл Катунду (2) г-жа Мвенде Нджираини (3) | г-н Эльхадж Мохамед М.К.(2)г-н Мвесигва Патрик (2)г-н Туре Мохамед (2) |
| РегГр-АРБ ИК17 | г-жа Уала Тюрки Латрус (4)г-н Бадар Али Саид Аль-Салехи (5) | г-жа Абделькадер Манель (6)г-жа Абуш Шехразед (6)г-жа Альмансури Лайаль (7) |
| Проект ASN.1 | Руководитель проекта: г-н Пол Торп |  |
| Проект OID | Руководитель проекта: г-н Оливье Дюбюиссон |  |
| Примечания:  (1) Сопредседатель с марта 2017 года.  (2) Председатель/заместитель председателя до сентября 2018 года.  (3) Председатель с апреля 2019 года.  (4) Сопредседатель с декабря 2017 года до октября 2018 года.  (5) (Со)Председатель с декабря 2017 года.  (6) Заместитель председателя с декабря 2017 до октября 2018 года.  (7) Заместитель председателя с декабря 2017 года.  (8) Исполняющий обязанности сопредседателя с апреля 2021 года. | | |

## 2.2 Вопросы и Докладчики

**2.2.1** ВАСЭ-16 поручила 17-й Исследовательской комиссии следующие 12 Вопросов, которые перечислены в Таблице 4, а также ИК17 назначила перечисленных Докладчиков и ассоциированных Докладчиков на настоящий исследовательский период.

ТАБЛИЦА 5

17-я Исследовательская комиссия – Вопросы, порученные ВАСЭ-16, и Докладчики (2017−2020 гг.)

| Вопросы | Название Вопроса | РГ | Докладчик (19) |
| --- | --- | --- | --- |
| Вопрос 1/17 | Координация деятельности в области безопасности электросвязи/ИКТ | PLEN | г-жа Латрус Уала (Докладчик) (13)г-н Эльхадж Мохамед M. K. (Докладчик) (1) г-жа Ки Джухи (ассоциированный Докладчик) (2) г-н Нажарян Пол (ассоциированный Докладчик) (3) г-н Сенга Ватару (ассоциированный Докладчик) (3) г-жа Ван Ивэнь (ассоциированный Докладчик) (3) |
| Вопрос 2/17 | Архитектура и структура безопасности | РГ 1/17 | г-жа Ху Чжиюань (Содокладчик) (3) г-н О Хён Рён (Содокладчик) (3)г-жа Шаабан Эмна (ассоциированный Докладчик) (10)г-н Ли Джин Мён (ассоциированный Докладчик) (16) |
| Вопрос 3/17 | Управление безопасностью информации, передаваемой по системам электросвязи | РГ 1/17 | г-жа Наганума Михо (Докладчик) (3) г-н Минь Цзинхуа (ассоциированный Докладчик) (7) г-н Мустафа Таиб (ассоциированный Докладчик) (5)г-н Фишер Андрес (ассоциированный Докладчик) (4) |
| Вопрос 4/17 | Кибербезопасность | РГ 2/17 | г-н Кадобаяси Юки (Докладчик) (6) г-н Ким Чон Юн (Докладчик) (7) г-н Сим Дон-Хи (ассоциированный Докладчик) (2) г-н Чжан Чень (ассоциированный Докладчик) (15)г-н Касановас Эдуардо (ассоциированный Докладчик) (4) |
| Вопрос 5/17 | Противодействие распространению спама техническими средствами | РГ 2/17 | г-н Чжан Яньбинь (Докладчик) (3) г-н Ким Чанг О (ассоциированный Докладчик) (3) |
| Вопрос 6/17 | Аспекты безопасности услуг и сетей электросвязи, а также интернета вещей (17) | РГ 1/17 | г-н Пэк Джонхён (Содокладчик) (3) г-жа Цзуо Минь (Содокладчик) (14)г-н Янь Цзюньчжи (Содокладчик) (8) г-н Ли Гонхи (ассоциированный Докладчик) (9) г-н Такахаси Такэси (ассоциированный Докладчик) (3) г-н Юй Бо (ассоциированный Докладчик) (3)г-жа Пасо-Роблес Мария Эухения (ассоциированный Докладчик) (4) |
| Вопрос 7/17 | Безопасные прикладные услуги | РГ 3/17 | г-н На Джэ Хун (Докладчик) (3) г-жа Гао Фэн (ассоциированный Докладчик) (7) г-н Лю Лицзюнь (ассоциированный Докладчик) (3) |
| Вопрос 8/17 | Безопасность облачных вычислений и инфраструктуры больших данных(18) | РГ 3/17 | г-н Вэй Лян (Докладчик) (3) г-н Ли Сан У (ассоциированный Докладчик) (9)г-н Макфадден Марк (ассоциированный Докладчик) (5) |
| Вопрос 9/17 | Телебиометрия | РГ 4/17 | г-н Карас Джон Джордж (Докладчик) (3)г-н Ли Кэпэн (ассоциированный Докладчик) (11)г-жа Ван Мэньси (ассоциированный Докладчик) (12) |
| Вопрос 10/17 | Архитектура и механизмы управления определением идентичности | РГ 4/17 | г-н Барбир Эбби (Докладчик) (3) г-н Парк Кындуг (ассоциированный Докладчик) (3) г-н Такети Хироси (ассоциированный Докладчик) (3) г-н Ся Цзюньцзе (ассоциированный Докладчик) (3) |
| Вопрос 11/17 | Общие технологии (справочник, инфраструктура открытых ключей (PKI), инфраструктура управления привилегиями (PMI), абстрактная синтаксическая нотация № 1 (ASN.1), идентификаторы объектов (OID)), поддерживающие безопасные приложения | РГ 4/17 | г-н Лемэр Жан-Поль (Докладчик) (3)г-жа Каддаши Ольфа (ассоциированный Докладчик) (18) |
| Вопрос 12/17 | Формальные языки для программного обеспечения систем электросвязи и тестирования | РГ 3/17 | г-н Хогриф Дитер (Докладчик) (3) г-н Муссбахер Гюнтер (ассоциированный Докладчик) (5)г-н Дуальде Мартин (ассоциированный Докладчик) (4) |
| (1) Назначен 5 сентября 2019 года.  (2) Назначен 30 января 2019 года.  (3) Назначен 30 марта 2017 года.  (4) Назначен 30 марта 2017 года, освобожден от должности 29 марта 2018 года.  (5) Назначен 6 сентября 2017 года.  (6) Назначен 30 марта 2017 года, полномочия прекращены (назначен повторно) (переназначен) 29 марта 2018 года.  (7) Назначен 29 марта 2018 года.  (8) Назначен 30 января 2019 года.  (9) Назначен 7 сентября 2018 года.  (10) Назначен 30 марта 2017 года, освобожден от должности 7 сентября 2018 года.  (11) Назначен 30 марта 2017 года, подал в отставку 7 сентября 2018 года.  (12) Назначен 6 сентября 2017 года, освобожден от должности 7 сентября 2018 года.  (13) Назначен 30 марта 2017 года, освобожден от должности в январе 2019 года.  (14) Назначен 29 марта 2018 года, подал в отставку 30 января 2019 года.  (15) Назначен 7 сентября 2018 года.  (16) Назначен 6 сентября 2017 года, освобожден от должности 7 сентября 2018 года.  (17) Название Группы Докладчика по Вопросу 6/17 "Аспекты безопасности услуг и сетей электросвязи" было изменено на "Аспекты безопасности услуг и сетей электросвязи, а также интернета вещей".  (18) Название Группы Докладчика по Вопросу 8/17 "Безопасность облачных вычислений" было изменено на "Безопасность облачных вычислений и инфраструктуры больших данных".  (19) Назначение действительно до 20 апреля 2021 года. | | | |

**2.2.2** В связи с переносом ВАСЭ-20 на март 2022 года собрание КГСЭ, состоявшееся 11−18 января 2021 года, одобрило новый комплекс из 12 Вопросов , перечисленных в Таблице 5a, которые были согласованы ИК17 на собрании ИК17 в августе/сентябре 2020 года (см. [Циркуляр 295](https://www.itu.int/md/T17-TSB-CIR-0295/en) БСЭ).

ТАБЛИЦА 5a

17-я Исследовательская комиссия – Вопросы, одобренные КГСЭ (с 18 января 2021 г.)

| Новый номер | Действующее название  Вопроса | Статус | Прежний номер | Прежнее название  Вопроса | РГ | Докладчик (1) |
| --- | --- | --- | --- | --- | --- | --- |
| 1/17 | Стратегия и координация стандартизации в области безопасности | Продолжен | 1/17 | Координация деятельности в области безопасности электросвязи/ИКТ | РГ 1/17 | Содокладчики:  − г-н Эльхадж Мохамед М.К. − г-жа Ки Джухи  Ассоциированные Докладчики:  − г-н Нажарян Пол − г-н Сенга Ватару Wataru − г-жа Ван Ивэнь |
| 2/17 | Архитектура безопасности и безопасность сетей | Продолжен | 2/17 | Архитектура и структура безопасности | РГ 2/17 | Содокладчики  − г-жа Ху Чжиюань − г-н О Хён Рён |
| 3/17 | Управление безопасностью информации, передаваемой с помощью электросвязи, и услуги по обеспечению безопасности | Продолжен | 3/17 | Управление безопасностью информации, передаваемой по системам электросвязи | РГ 3/17 | Докладчик:  − г-жа Наганума Михо  Ассоциированные Докладчики:  − г-н Минь Цзинхуа − г-н Мустафа Таиб |
| 4/17 | Кибербезопасность и противодействие спаму | Продолжение Вопросов 4/17 и 5/17 | 4/17 | Кибербезопасность | РГ 3/17 | Содокладчики:  − г г-н Ким Чон Юн − г-н Чжан Яньбинь  Ассоциированные Докладчики:  − г-н Ким Чанг О |
| 5/17 | Противодействие распространению спама техническими средствами |
| 6/17 | Безопасность услуг электросвязи и интернета вещей | Продолжен | 6/17 | Аспекты безопасности услуг, сетей электросвязи и интернета вещей | РГ 2/17 | Содокладчики:  − г-н Пэк Джонхён − г-н Янь Цзюньчжи  Ассоциированные Докладчики:  − г-н Ли Гонхи  − г-н Такахаси − г-н Юй Бо |
| 7/17 | Безопасные прикладные услуги | Продолжен | 7/17 | Безопасные прикладные услуги | РГ 4/17 | Докладчик:  − г-н На Джэ  Ассоциированные Докладчики:  − г-жа Гао Фэн − г-н Лю Лицзюнь |
| 8/17 | Безопасность облачных вычислений и инфраструктуры больших данных | Продолжен | 8/17 | Безопасность облачных вычислений и инфраструктуры больших данных | РГ 4/17 | Докладчик:  − г-н Вэй Лян  Ассоциированные Докладчики:  − г-н Макфадден Марк |
| 10/17 | Архитектура и механизмы управления определением идентичности и телебиометрии | Продолжение Вопросов 9/17 и 10/17 | 9/17 | Телебиометрия | РГ 5/17 | Содокладчики:  − г-н Барбир Эбби − г-н Карас Джон Джордж  Ассоциированные Докладчики:  − г-н Ким Джейсон − г-н Парк Кындуг − г-н Такети Хироси − г-н Ся Цзюньцзе |
| 10/17 | Архитектура и механизмы управления определением идентичности |
| 11/17 | Общие технологии (например, Справочник, PKI, формальные языки, идентификаторы объекта) для поддержки безопасных приложений | Продолжение Вопросов 11/17 и 12/17 | 11/17 | Общие технологии (Справочник, инфраструктура открытых ключей (PKI), инфраструктура управления привилегиями (PMI), абстрактная синтаксическая нотация № 1 (ASN.1), идентификаторы объектов (OID)) для поддержки безопасных приложений | РГ 5/17 | Докладчик:  − г-н Лемэр Жан-Поль  Ассоциированный Докладчик:  − г-н Хогриф Дитер |
| 12/17 | Формальные языки для программного обеспечения систем электросвязи и тестирования |
| 13/17 | Безопасность интеллектуальных транспортных систем (ИТС) | Продолжен | 13/17 | Аспекты безопасности интеллектуальных транспортных систем | РГ 2/17 | Докладчик:  − г-н Ли Сан У  Ассоциированные Докладчики:  − г-н Пак Сынук  − г-жа Чжан И |
| 14/17 | Безопасность технологии распределенного реестра (DLT) | Продолжен | 14/17 | Аспекты безопасности технологий распределенного реестра | РГ 4/17 | Содокладчики:  − г-н Кадобаяси Юки − г-жа О Кён Хи  Ассоциированные Докладчики: − г-жа Бай Сяоюань − г-жа Ван Кэ |
| 15/17 | Безопасность для/с помощью появляющихся технологий, включая квантовую безопасность | Новый | – | – | РГ 1/17 | Докладчик:  − г-н Сим Дон-Хи  Ассоциированные Докладчики:  − г-н Кеноси Каору  − г-н Юн Чун Сок − г-н Чжан Чень |
| (1) Назначен (повторно назначен) на собрании ИК17 20−30 апреля 2021 года. | | | | | | |

**2.2.3** Вопросы, перечисленные в Таблице 5b, были приняты заново в течение этого периода.

ТАБЛИЦА 5b

17-я Исследовательская комиссия – Принятые новые Вопросы и Докладчики

| Вопросы | Название Вопроса | РГ | Докладчик |
| --- | --- | --- | --- |
| Вопрос 13/17 | Аспекты безопасности для интеллектуальной транспортной системы (10)/ Безопасность интеллектуальной транспортной системы (ИТС) (11) | РГ 1/17 (10) / РГ 2/17 (11) | г-н Ли Сан У (Докладчик)(1) г-н Пак Сынук (ассоциированный Докладчик)(1) г-жа И Чжан (ассоциированный Докладчик)(2) |
| Вопрос 14/17 | Аспекты безопасности технологий распределенного реестра (10)Безопасность технологии распределенного реестра (DLT) (11) | РГ 2/17 (10) / РГ 3/17 (11) | г-н Кадобаяси Юки (Содокладчик)(3) г-жа О Кён Хи (Содокладчик)(3) г-жа Бай Сяоюань (ассоциированный Докладчик)(4) г-жа Ван Кэ (ассоциированный Докладчик)(4)  г-жа Цзуо Минь (ассоциированный Докладчик)(5) |
| Вопрос 15/17 | Безопасность для/с помощью появляющихся технологий, включая квантовую безопасность | РГ 1/17 (11) | г-н Сим Донг-хи (Докладчик)(6)  г-н Кеноси Каору (ассоциированный Докладчик)(7)  г-н Юн Чун Сок (ассоциированный Докладчик) (8)  г-н Чжан Чень (ассоциированный Докладчик)(9) |
| (1) Назначен 30 марта 2017 года.  (2) Назначен 7 сентября 2018 года.  (3) Назначен 6 сентября 2017 года.  (4) Назначен 29 марта 2018 года.  (5) Назначен 6 сентября 2017 года, полномочия прекращены (назначен повторно) (переназначен) 29 марта 2018 года.  (7) Назначен 20 апреля 2021 года  (8) Назначен 20 апреля 2021 года, ответственный .  (9) Назначен 20 апреля 2021 года  (10) 2017−2020 гг.  (11) 2021−2022 гг. | | | |

**2.2.4** В течение данного периода Вопросы, перечисленные в Таблице 6, были включены в другие Вопросы ИК17.

ТАБЛИЦА 6

17-я Исследовательская комиссия – Исключенные Вопросы

| Вопросы | Название Вопроса | Докладчик | Результаты |
| --- | --- | --- | --- |
| Вопрос 5/17 (исключен) | Противодействие распространению спама техническими средствами | г-н Чжан Яньбинь (Докладчик) г-н Ким Чанг О (ассоциированный Докладчик) | Вопрос 5/17 объединен с Вопросом 4/17 18 января 2021 г. после одобрения объединения со стороны КГСЭ |
| Вопрос 9/17 (исключен) | Телебиометрия | Карас Джон Джордж (Докладчик) | Вопрос 9/17 объединен с Вопросом 10/17 18 января 2021 г. после одобрения объединения со стороны КГСЭ |
| Вопрос 12/17 (исключен) | Формальные языки для программного обеспечения систем электросвязи и тестирования | г-н Хогриф Дитер (Докладчик) г-н Муссбахер Гюнтер (ассоциированный Докладчик) | Вопрос 12/17 объединен с Вопросом 11/17 18 января 2021 г. после одобрения объединения со стороны КГСЭ |

# 3 Результаты работы, завершенной в течение исследовательского периода 2017−2020 годов

## 3.1 Общая информация

В течение рассматриваемого исследовательского периода до своего электронного собрания, состоявшегося 7 января 2022 года, 17‑я Исследовательская комиссия изучила большое количество вкладов, временных документов (TD) и заявлений о взаимодействии.

На основе этих документов к 7 января 2022 года 17-я Исследовательская комиссия:

– разработала 53 новых Рекомендаций в рамках АПУ + 47 новых Рекомендаций в рамках ТПУ; (по трем Рекомендациям в рамках ТПУ сделано заключение);

– пересмотрела 93 существующих Рекомендаций в рамках АПУ + три существующих Рекомендации в рамках АПУ;

– внесла изменения в четыре Рекомендации;

– разработала восемь новых Добавлений, одно пересмотренное Добавление и одно Исправление к одному существующему Добавлению;

– выпустила 17 Технических исправлений;

− разработала два новых Технических документа и шесть Технических отчетов (Справочников подготовлено не было).

В течение рассматриваемого исследовательского периода до своего электронного собрания, состоявшегося 7 января 2022 года, 17‑я Исследовательская комиссия:

– привлекла 2163 (2063+100) участников (в разбивке по прошедшим собраниям: 100, 223, 231, 91, 262, 69, 225, 206, 178, 168, 130, 134, 146);

– создала 162 новых направления работы (в разбивке по прошедшим собраниям: 7, 15, 0, 15, 7, 26, 13, 25, 21, 26, 7);

– получила 1179 вкладов (в разбивке по прошедшим собраниям: 1, 98, 104, 2, 110, 121, 151, 118, 144, 113, 106, 78);

– выпустила 4220 временных документов (в разбивке по прошедшим собраниям: 106, 336, 305, 44, 434, 35, 439, 508, 380, 420, 395, 426, 368);

– получила 585 входящих заявлений о взаимодействии и выпустила 328 исходящих заявления о взаимодействии (в разбивке по прошедшим собраниям: 55+1, 51+23, 36+17, 21+0, 58+32, 1+2, 77+24, 64+42, 47+30, 40+37, 46+37, 49+40, 40+38).

## 3.2 Важнейшие результаты деятельности

Ниже кратко представлены основные достигнутые результаты в исследовании различных Вопросов, порученных 17-й Исследовательской комиссии.

Официальные ответы на Вопросы представлены в сводной таблице, содержащейся в Приложении 1 к настоящему отчету.

### а) Вопрос 1/17 − Координация деятельности в области безопасности электросвязи/ИКТ (2017−2020 гг.)/Стратегия и координация стандартизации в области безопасности (2021 г. −)

Группа Докладчика по Вопросу 1/17 является координатором ИК17 и координирует работу в области безопасности электросвязи/ИКТ, проводимую как внутри ИК17, так и в сотрудничестве с другими исследовательскими комиссиями и внешними организациями. В рамках Вопроса 1/17 также осуществляется разработка и ведение нескольких информационно-пропагандистских и справочных документов, которые МСЭ-T считает ценными для пропаганды своей работы в области безопасности и ее результатов. Например:

– Руководство по безопасности "Безопасность в электросвязи и информационных технологиях – Обзор содержания и применения действующих Рекомендаций МСЭ-Т для обеспечения защищенной электросвязи" содержит информацию об основной деятельности в области безопасности исследовательских комиссий МСЭ-Т. В течение рассматриваемого исследовательского периода Группа Докладчика по Вопросу 1/17 подготовила седьмое издание.

– Технический отчет об эффективном использовании стандартов безопасности способам эффективного применения утвержденных Рекомендаций МСЭ-Т, связанных с безопасностью. Рассматриваются как отдельные Рекомендации (например, МСЭ-T X.805), так и серии Рекомендаций (например, CYBEX), а также потенциальные выгоды, которые может принести их использование. В течение рассматриваемого исследовательского периода Группа Докладчика по Вопросу 1/17 подготовила второе издание.

− Дорожная карта по стандартам в области безопасности ИКТ содержит онлайновую базу данных с возможностью поиска, в которой собрано более 2600 утвержденных стандартов в области безопасности ИКТ, разработанных исследовательскими комиссиями МСЭ-T и внешними организациями по разработке стандартов (ОРС), в том числе 3D@home, 3GPP, 3GPP2, ATIS, ЕТСИ, IEEE, IETF, ОТК1 ИСО/МЭК, OASIS, oneM2M, SmartBan и TETRA. В течение рассматриваемого исследовательского периода Группа Докладчика по Вопросу 1/17 утвердила большое число обновлений.

− В Сборнике Рекомендаций по безопасности в части I содержится каталог утвержденных Рекомендаций МСЭ-Т, касающихся безопасности электросвязи, а в части II – выдержки из утвержденных МСЭ-Т определений в области безопасности. В течение рассматриваемого исследовательского периода Сборник обновлялся на каждом собрании Группы Докладчика по Вопросу 1/17.

Была налажена координация деятельности со всеми Группами Докладчиков по Вопросам 17‑й Исследовательской комиссии, со всеми другими исследовательскими комиссиями, занимающимися вопросами безопасности, а также с внешними организациями по разработке стандартов, участвующими в работе, связанной со стандартами безопасности ИКТ.

Группа Докладчика по Вопросу 1/17 также содействовала проведению семинаров-практикумов по безопасности, оказала помощь двум региональным группам ИК17 (для Африки и для арабских государств) и повысила эффективность работы ИК17 путем создания шаблонов, инструментов и разработки процедур. По состоянию на конец 2021 года Группа Докладчика по Вопросу 1/17 течение рассматриваемого исследовательского периода оказала МСЭ помощь в проведении 13 семинаров-практикумов МСЭ.

### b) Вопрос 2/17 − Архитектура и структура безопасности (2017−2020 гг.)/Архитектура безопасности и безопасность сетей (2021 г. −)

В рамках Вопроса 2/17 разрабатывается всеобъемлющий набор Рекомендаций по вопросам архитектуры и структуры безопасности для предоставления стандартных решений по обеспечению безопасности электросвязи. Это включает безопасность для 5G, структуры безопасности сетей с программируемыми параметрами, передача голоса на основе технологии долгосрочного развития и виртуализация сетей.

В течение рассматриваемого исследовательского периода в рамках Вопроса 2/17 разработаны восемь новых Рекомендаций и одно новое Добавление:

– X.1011, *Руководящие указания по обеспечению непрерывной защиты процесса доступа к услуге*, где проводится анализ угроз безопасности процесса доступ к *услуге*, определяются меры защиты безопасности для обнаружения анормальных действий доступа и вводится усовершенствованный механизм авторизации для доступа к услуге.

− X.1040, *Эталонная архитектура безопасности для управления жизненным циклом бизнес-данных электронной коммерции*, где проводится анализ основных свойств и типовых угроз, с которыми сталкиваются экосистемы услуг электронной коммерции, и представлена эталонная архитектура безопасности для управления на протяжении жизненного цикла бизнес-данными электронной коммерции.

− X.1041, *Структура безопасности работы сети для передачи голоса на основе технологии долгосрочного развития (VoLTE)*, где проводится анализ угроз безопасности, возникающих в сети VoLTE, и представлены предназначенные для операторов электросвязи рекомендации по мерам противодействия, позволяющие обеспечивать безопасную работу. Также представлена эталонная структура безопасности для сети VoLTE.

– X.1043, *Структура и требования безопасности для создания цепочек функций услуг на базе сетей с программируемыми параметрами*,где представленанализ угроз безопасности и указаны требования безопасности для создания цепочек функций услуг на базе сетей с программируемыми параметрами (SDN). Также приведены соответствующие контрмеры в сфере безопасности. Цель Рекомендации МСЭ-T X.1043− содействие осмыслению рисков безопасности, возникающих при создании цепочек функций услуг на базе SDN, и создание безопасных цепочек функций услуг на базе SDN.

– X.1044, *Требования безопасности виртуализации сетей*,где представлен анализпроблем и угроз безопасности, связанных с виртуализацией сети (NV), и определены требования к безопасности для уровня физических ресурсов, уровня виртуальных ресурсов и уровня логически изолированных участков сети (LINP) в среде виртуализации сети.

– X.1045, *Архитектура цепочки услуг безопасности для сетей и приложений*,которая служит для поддержки предоставления специализированных динамических и адаптивных услуг безопасности для сетей и приложений. В настоящей Рекомендации описана цепочка услуг безопасности и проектирование архитектуры для цепочки услуг безопасности. В настоящей Рекомендации описано применение цепочки услуг безопасности для сетей и приложений. Настоящая Рекомендация обеспечивает также возможность отслеживания атак на сетевые ресурсы в высокопроизводительной оверлейной сети цепочек функций услуг (SFC) и автоматического смягчения последствий/предупреждения атак.

– X.1046, *Структура безопасности с программируемыми параметрами в сетях с программируемыми параметрами/сетях с виртуализацией сетевых функций*, где определена структура безопасности с программируемыми параметрами – в сетях с программируемыми параметрами (SDN) и в сетях с виртуализацией сетевых функций (NFV). В настоящей Рекомендации анализируются основные проблемы безопасности, в том числе технические и эксплуатационные аспекты сетей операторов на базе технологий SDN/NFV. В настоящей Рекомендации определяются требования к безопасности для решения этих проблем в сетях SDN/NFV. В настоящей Рекомендации вводится понятие "безопасность с программируемыми параметрами" и разрабатывается структура безопасности с программируемыми параметрами. В настоящей Рекомендации описывается реализация безопасности с программируемыми параметрами.

– X.1047, *Требования и архитектура безопасности для управления отрезками сети и их оркестровки,* где устанавливаются требования и архитектура безопасности для управления отрезками сети и их оркестровки, а также автоматическое создание сквозных отрезков сети (E2E) с настраиваемыми средствами безопасности, для развертывания полномасштабной E2E сетевой нарезки для потребительского, делового и государственного сегментов.

– X.Suppl 30, *МСЭ-T X.805 – Руководство по безопасности для оператора виртуальной сети подвижной связи*,гдесодержится руководство по безопасности для оператора виртуальной сети подвижной связи (MVNO). Безопасность очень важна для MVNO, и у большинства MVNO есть много общего в плане безопасности. В настоящем Добавлении анализируются основные характеристики MVNO и типичные угрозы безопасности, с которыми они сталкиваются. В настоящем Добавлении излагается структура безопасности для MVNO, выстроенная на базе структуры MVNO, в том числе задачи в области безопасности и требования к безопасности.

### c) Вопрос 3/17 − Управление безопасностью информации, передаваемой по системам электросвязи (2017−2020 гг.)/Управление безопасностью информации, передаваемой с помощью электросвязи, и услуги по обеспечению безопасности (2021 г. −)

В рамках Вопроса 3/17 разрабатываются Рекомендации по управлению безопасностью информации электросвязи, например свод правил в отношении информации, позволяющей установить личность (PII), для организаций электросвязи и для малых и средних организаций электросвязи.

В течение рассматриваемого исследовательского периода в рамках Вопроса 3/17 разработано пять новых Рекомендаций, одно Исправление, два пересмотренных и три новых Добавления:

− Исправление к Рекомендации X.1051 (пересмотренной), *Информационные технологии – Методы обеспечения безопасности – Руководящие указания по управлению информационной безопасностью для организаций электросвязи, основанные на стандарте ИСО/МЭК 27002*.

– X.1052 (пересмотренная), *Процессы управления информационной безопасностью для организаций электросвязи,* где представлен передовой опыт управления информационной безопасностью для организаций электросвязи с целью поддержки Рекомендации МСЭ-T X.1051. Настоящая Рекомендация основана на концепции процессов для описания набора областей управления безопасностью, которые формируют рекомендации для организаций электросвязи по осуществлению задач управления, определенных в Рекомендации МСЭ-Т X.1051. Описанные в настоящей Рекомендации области управления, включая управление ресурсами, управление инцидентами, управление рисками, управление политикой, и осуществляют отображение средств управления, определенных в Рекомендации МСЭ-Т X.1051, для реализации методики.

– X.1053, *Свод правил по управлению информационной безопасностью на основе МСЭ-T X.1051 для малых и средних организаций электросвязи*,где установлены руководящие указания и общие принципы инициирования, реализации, сопровождения и совершенствования средств управления информационной безопасностью в малых и средних организациях электросвязи (SMTO) на основе МСЭ-T X.1051. В настоящей Рекомендации представлены также базовые параметры внедрения средств управления информационной безопасностью в CMTO, для того чтобы обеспечить конфиденциальность, целостность и доступность средств и услуг электросвязи, а также информации, которая передается, обрабатывается или хранится с использованием этих средств и услуг.

– X.1058, *Информационные технологии – Методы обеспечения безопасности – Свод правил и норм для защиты информации, позволяющей установить личность*,гдеустанавливаются задачи управления, средства управления для решения данных задач исходя из требований, выработанных по результатам оценки риска и анализа последствий для защиты PII, а также руководящие указания по реализации этих средств управления. В частности, настоящая Спецификация содержит руководящие указания на базе стандарта ИСО/МЭК 27002 с учетом требований к обработке PII, которые могут быть применимы в контексте свойственной организации среды рисков нарушения информационной безопасности.

– X.1059, *Руководство по внедрению в организациях электросвязи управления рисками в отношении своих активов, доступных по глобальным сетям на базе IP*,гдеприведено руководство для организаций электросвязи по управлению рисками в отношении своих активов, доступных по глобальным сетям на базе IP, то есть активов, которые непосредственно подвергаются воздействию хакеров и злоумышленников. Эти активы могут быть также соединены с традиционными (или даже старыми) активами унаследованных сетей электросвязи, возможно содержащими определенные уязвимости на уровне проектного решения, которые сложно устранить. Следовательно, было бы целесообразно рассматривать все активы организации электросвязи, доступные по глобальным сетям на базе IP (AGIT), как единое целое и вводить определенные конкретные средства безопасности в целях непрерывного снижения общих рисков и укрепления общей безопасности услуг и сетей электросвязи.

– X.1060, *Структура для создания и эксплуатации центра по защите от киберугроз,* гдецентр по защите от киберугроз (CDC) определен как подразделение, которому отведена центральная роль в обеспечении противодействия рискам кибербезопасности в организации. Структура описана как три процесса – построение, управление и оценка, которые CDC должен реализовать на практике. Описаны также услуги, которые должна предусмотреть организация для принятия более конкретных мер кибербезопасности.

– X.1061, *Руководство по приобретению киберстрахования для поставщиков услуг информационно-коммуникационных технологий (ИКТ)*

Это руководство по приобретению киберстрахования обеспечивает понимание покрытия киберстрахования и требований к оценкам рискам кибербезопасности, выбору страховщика, оценкам, проводимым страховщиком, и оценке страховщика для организаций, которые принимают киберстрахование как вариант регулирования рисков для управления последствиями инцидента в области кибербезопасности.

– X.Suppl.13 (пересмотренное), *МСЭ-T X.1051 − Руководство для пользователей по управлению информационной безопасностью*.

– X.Suppl.32, *МСЭ-T X.1058 − Свод правил и норм для защиты информации, позволяющей установить личность,* *для организаций электросвязи*,гдепредставлена информация, дополняющая информацию в МСЭ-T X.1058, в виде дополнительных руководящих указаний по реализации защиты информации, позволяющей установить личность (PII), которые не излагаются в МСЭ-T X.1058 и в дальнейшем должны применяться организациями электросвязи для защиты PII.

– X.Suppl.34, *МСЭ-T X.1051 − Руководство для пользователей по управлению информационной безопасностью для организаций электросвязи*,гдепредставлена информация о выполнении Руководства по управлению информационной безопасностью и безопасностьюсетей предприятиями отрасли информационно-коммуникационных технологий Малайзии на основе Рекомендации МСЭ-T X.1051.

– X.Suppl.36, *ITU-T X.1051 – Важнейшие меры по обеспечению безопасности для управления информационной и сетевой безопасностью организаций электросвязи*, где представлен передовой опыт обеспечения кибербезопасности для управления безопасностью с использованием важнейших мер по обеспечению безопасности в рамках сферы применения Рекомендации МСЭ-T X.1051. Использование структуры важнейших мер по обеспечению безопасности (CSC) и соответствующих важнейших мер безопасности поддерживает и дополняет Рекомендацию МСЭ-T X.1051.

В рамках Вопроса 3/17 налажено тесное сотрудничество с РГ1 ПК27 ОТК1 ИСО/МЭК по вопросам управления информационной безопасностью.

### d) Вопрос 4/17 − Кибербезопасность (2017−2020 гг.)/Кибербезопасность и противодействие спаму (2021 г. −)

В рамках Вопроса 4/17 разрабатываются Рекомендации по структурам кибербезопасности и требованиям к тому, как поставщики услуг электросвязи/ИКТ должны защищать свою инфраструктуру и поддерживать безопасность операций, а также обмениваться информацией о кибербезопасности. В данном исследовательском периоде в сферу охвата Вопроса 4/17 до 2020 года была также включена функция инкубатора для рассмотрения возникающих вопросов, таких как безопасность в квантовой среде, и эта функция была передана в Вопрос 15/17 в январе 2021 года. Также в январе 2021 года Вопрос 4/17 принял текущую работу по противодействию спаму, ранее выполняемую в рамках исследований по Вопросу 5/17.

В течение рассматриваемого исследовательского периода в рамках Вопроса 4/17 разработаны 14 новых Рекомендаций, одна пересмотренная Рекомендация, две новые Поправки, два новых Технических документа и два новых Технических отчета:

− X.1212, *Проектные решения для улучшенного восприятия конечным пользователем показателей благонадежности*, где представлены проектные решения для улучшенного восприятия конечным пользователем показателей благонадежности. В дополнениях описываются типичные методы измерения восприятия конечным пользователем таких показателей.

− X.1213, *Требования к возможностям обеспечения безопасности для противодействия бот-сетям, использующим смартфоны*,где представлен анализ текущей ситуации и потенциальных угроз безопасности со стороны бот-сетей, использующих смартфоны, а также требования к возможностям обеспечения безопасности.

− X.1214, *Методы оценки безопасности в сетях электросвязи/информационно-коммуникационных технологий*,где приведено описание методики оценки безопасности элементов программного обеспечения сетей электросвязи/информационно-коммуникационных технологий (ИКТ) и примеров передового опыта для использования разработчиками, производителями, операторами и экспертами по безопасности в области электросвязи при решении вопросов безопасности соответствующих элементов программного обеспечения. Как традиционные сети с коммутацией каналов, так и пакетные сети подвержены различным угрозам и атакам, исходящим из внешних и внутренних источников и нацеленным на различные части сети электросвязи/ИКТ. Настоящая Рекомендация охватывает как обнаружение уязвимостей в сетях электросвязи/ИКТ, так и методику оценки безопасности в сетях электросвязи/ИКТ.

− X.1215, *Сценарии использования структурированного представления информации об угрозах*,где представлены различные сценарии возможного использования языка структурированного представления информации об угрозах (STIX) в поддержку сбора оперативной информации об угрозах (CTI) и совместного использования этой информации.

− X.1216, *Требования к сбору и сохранению доказательств по инцидентам кибербезопасности*,гдеописана общая процедура реагирования на инциденты кибербезопасности и их расследования. Также проведен анализ источников доказательств по инцидентам кибербезопасности и определены требования к возможностям инструментов, используемых для сбора и сохранения таких доказательств в процессе расследования. Наряду с этим в настоящей Рекомендации определены требования к гарантированию надежности этих инструментов в форме руководства для разработчиков, проектирующих такие инструменты для этих целей.

– X.1217, *Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи*. Для оператора электросвязи оперативная информация об угрозах – это совокупность систематизированной, проанализированной и уточненной информации о потенциальных и текущих атаках, которые могут угрожать организации. Эта информация может включать также данные о мотивах, намерениях, характеристиках и методах злоумышленников, наряду со сведениями об их образе или методах действия, тактике и процедурах. В сфере сетевой и информационной безопасности возникновение крупномасштабных и неожиданных нарушений кибербезопасности обусловило неотложную потребность в оперативной информации об угрозах. Оперативная информация об угрозах может помочь организации снизить риски и повысить общий уровень безопасности. Для того чтобы обеспечить возможность обмена оперативной информацией об угрозах между различными организациями, определены унифицированные классификация, грамматика и представление оперативной информации об угрозах. В настоящей Рекомендации представлены руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи после обзорного анализа.

– X.1218, *Требования и руководящие указания по динамическому анализу вредоносного программного обеспечения в изолированной среде*. В сложных атаках, в особенности при реализации постоянных устойчивых угроз (APT), для того чтобы не допустить обнаружения, обычно используется неизвестное вредоносное программное обеспечение. Например, целевая атака с фишинговой электронной почтой, в которой в качестве оружия применяется неизвестное вредоносное программное обеспечение, может легко осуществить успешное начальное нарушение. Таким образом, для обнаружения сложных атак следует уделять особое внимание обнаружению неизвестных программ и принимать для этого специальные меры защиты. В Рекомендации МСЭ-T X.1218 приведен анализ угроз, связанных с неизвестным программным обеспечением, и описаны требования по обнаружению неизвестного программного обеспечения, основанные на динамическом анализе поведения.

– X.1233, *Руководящие указания по противодействию распространению спама при мгновенном обмене сообщениями*, где определены предназначенные для поставщиков и пользователей услуг мгновенного обмена сообщениями (IM) руководящие указания по противодействию распространению спама при мгновенном обмене сообщениями (спим). Рассматриваются сценарии распространения спама при мгновенном обмене сообщениями; технические меры и механизмы противодействия спиму, предназначенные для поставщиков услуг IM, а также меры экстренного реагирования для противодействия спиму, предназначенные для пользователей IM, и т. д.

– X.1234, *Руководящие указания по противодействию распространению спама с использованием услуг передачи мультимедийных сообщений (MMS)*, где определены руководящие указания по противодействию распространению спама с использованием MMS. В ней анализируются типичные сценарии, характеристики и методы распознавания MMS‑спама, а также предоставлены техническая основа, рабочие процессы и некоторые ключевые технологии распознавания MMS-спама, которые помогут поставщикам и пользователям услуг MMS противодействовать спаму.

– X.1235, *Технологии противодействия подделке веб-сайтов, предназначенные для организаций электросвязи*, где организациям электросвязи рекомендуются технологии для своевременного выявления подделки веб-сайтов и защиты своих веб-сайтов от подделки.

− Поправки 11 и 12 к X.1500, *Обзор обмена информацией по кибербезопасности*,где представлен список методов обмена структурированной информацией о кибербезопасности, подготовленный в целях его непрерывного обновления по мере появления, расширения и замены таких методов или выявления новых методов. Список ведется на основе схемы, представленной в тексте Рекомендации. Отражена ситуация с рекомендованными методами, включая библиографические ссылки, по состоянию на март 2017 года и март 2018 года.

– X.1541 (пересмотренная), *Формат обмена описаниями инцидентов как объектов, версия 2*,гдепредставлена информационная модель формата обмена описаниями инцидентов как объектов (IODEF), версия 2, и приведена соответствующая модель данных в форме схемы XML. Формат IODEF определяет представление модели ‎данных для совместного использования информации, которой обычно обмениваются, об инцидентах, связанных с нарушением ‎компьютерной безопасности, или иных типах инцидентов. Для этого перечислены соответствующие пункты IETF RFC 7970 с указанием их характера – нормативного или информативного.

– X.1550, *Модели контроля доступа для сетей обмена информацией об инцидентах*,гдепредставлены существующие подходы к реализации политики контроля доступа для сетей обмена информацией об инцидентах. В настоящей Рекомендации представлены разнообразные уже установившиеся модели контроля доступа, модели обмена информацией, а также критерии для оценки показателей работы сетей обмена информацией об инцидентах. Рассматриваются основанные на стандартах решения, направленные на содействие реализации различных моделей контроля доступа в рамках различных моделей обмена информацией по вопросам кибербезопасности и в разных условиях среды доверия.

– X.1702, *Архитектура генератора случайных чисел квантового шума*,гдеопределена общая функциональная архитектура источника квантовой энтропии, общий метод оценки и проверки энтропии оцениваемого источника шума, а также общий метод описания экстрактов случайности, когда они являются частью реализованной системы.

– X.1710, *Структура безопасности сетей квантового распределения ключей*, где определена структура, включая требования и меры, для борьбы с угрозами безопасности для сетей квантового распределения ключей (QKDN). Описана упрощенная схема QKDN для анализа соответствующих угроз безопасности. Далее на этой основе определяются требования безопасности и соответствующие меры безопасности.

– X.1714, *Комбинация ключей и секретная доставка ключей для сетей квантового распределения ключей*, где описаны методы комбинирования ключей для сетей квантового распределения ключей (QKDN) и определены требования безопасности как для комбинации ключей, так и для доставки ключей от QKDN до криптографических приложений.

– TP.inno, *Описание механизма инкубации и способов его улучшения*, где полностью описан механизм инкубации, созданный ИК17. Далее перечислены другие способы и механизмы, используемые МСЭ и другими ОРС для принятия инноваций.

– TP.sgstruct, *Стратегические подходы к преобразованию исследований в области безопасности*, охватывает кратко-, средне- и долгосрочные аспекты преобразования исследований в области безопасности.

– TR.sec-qkd, *Вопросы безопасности для сетей квантового распределения ключей,* где разработана структура QKD для выполнения требований со стороны сети электросвязи.

– TR.usm, *Унифицированная модель безопасности (USM) – нейтральный интегрированный системный подход к кибербезопасности*, где представлена универсальная архитектура "все аспекты безопасности", которая является нейтральной и агностической. Она может упростить широкую функциональную совместимость средств контроля безопасности и автоматизировать меры реагирования в плане безопасности.

В течение данного исследовательского периода Группа Докладчика по Вопросу 4/17 года провела небольшой семинар-практикум по безопасной квантовой связи (Женева, 24 января 2019 г.).

### e) Вопрос 5/17 − Противодействие распространению спама техническими средствами (2017−2020 гг.)

В рамках Вопроса 5/17 разрабатываются Рекомендации по противодействию распространению спама техническими средствами, например противодействию рекламному спаму, спаму в службе мгновенных сообщений, рекламному спаму в приложениях для мобильных устройств, мерам противодействия атакам типа "фишинг" и "смишинг" через службу коротких сообщений, а также противодействию мошенничеству при предоставлении услуг телефонной связи.

В течение рассматриваемого исследовательского периода в рамках Вопроса 5/17 разработаны три новые Рекомендации и два новых Добавления:

− X.1232, *Техническая основа противодействия рекламному спаму в информации, генерируемой пользователями*, где проведен анализ сценариев и характеристик рекламного спама, а также определена эталонная структура и потоки процессов, с тем чтобы помочь поставщикам услуг интернета противодействовать рекламному спаму.

− X.1248, *Технические требования для противодействия распространению спама при мгновенном обмене сообщениями*,гдеопределены характеристики спама, распространяемого при мгновенном обмене сообщениями (спим), и описаны технические требования для противодействия спаму. С ростом популярности мгновенного обмена сообщениями распространение спима становится все более серьезной проблемой. Характеристики мгновенного обмена сообщениями, такие как функционирование на базе протокола Интернет (IP) и широкое использование, за которое не взимается плата, потенциально способствуют масштабному и не поддающемуся контролю распространению спима. Проблему спима следует решать всесторонне, в противном случае он может оказать негативное воздействие на использование самой услуги мгновенного обмена сообщениями.

− X.1249, *Техническая основа противодействия рекламному спаму в приложениях для мобильных устройств*,где изложена техническая основа противодействия рекламному спаму в приложениях для мобильных устройств. Рекламный спам в приложениях для мобильных устройств – это рассылка нежелательной рекламы, которая отображается в приложении для мобильного телефона. Эта незапрашиваемая реклама может отображаться на экране мобильного устройства в виде баннера в верхней или нижней части экрана, подвижного окна или всплывающего окна.

– X.Suppl.29, *МСЭ-T X.1242 − Добавление, касающееся руководящих указаний по мерам противодействия атакам типа "фишинг" и "смишинг" через службу коротких сообщений (SMS)*,гдесодержатся универсальные руководящие указания по мерам противодействия атакам типа "фишинг" через службу коротких сообщений (SMS) – метод мошенничества с использованием мобильных телефонов, который делает возможным фишинговое мошенничество со смартфонами, получение личной информации в смартфонах или одобрение выплат на небольшую сумму и перевод соответствующих сумм, в то время как владелец счета не знает об одобрении.

– X.Suppl.33, *МСЭ-T X.1231 − Добавление, касающееся технической основы для противодействия мошенничеству в телефонных услугах*,гдеизлагается техническая основа и соответствующие примеры передового опыта противодействия мошенничеству в телефонных услугах. В рамках данной основы определены функции объектов и процедуры обработки. К числу примеров передового опыта отнесены те, которые считаются наиболее эффективными в борьбе с известными методами мошенничества в телефонных услугах.

### f) Вопрос 6/17 − Аспекты безопасности услуг и сетей электросвязи, а также интернета вещей (2017−2020 гг.)/Безопасность услуг электросвязи и интернета вещей (2021 г. −)

В рамках Вопроса 6/17 разрабатываются Рекомендации, касающиеся требований и структуры безопасности услуг электросвязи, сетей подвижной связи, "умных" электросетей, IPTV и интернета вещей.

В течение рассматриваемого исследовательского периода в рамках Вопроса 6/17 разработаны 17 новых Рекомендаций, одна Поправка и одно Исправление к существующему Добавлению:

– X.1042, *Службы безопасности, использующие сети с программируемыми параметрами*, которая касается защиты ресурсов сети с использованием служб безопасности на основе сетей с программируемыми параметрами (SDN). В настоящей Рекомендации сетевые ресурсы служб безопасности на основе SDN сначала классифицируются по следующим категориям: SDN-приложение, SDN-контроллер, SDN-коммутатор и диспетчер безопасности (SM). Затем в Рекомендации МСЭ-Т X.1042 дается определение конкретных служб безопасности на основе SDN.

– X.1126, *Руководящие указания по смягчению негативных последствий от зараженных терминалов в сетях подвижной связи*, гдесодержатся руководящие указания для операторов подвижной связи, призванные ограничить с помощью технологий использование зараженных терминалов в сетях подвижной связи, чтобы защитить как абонентов, так и операторов подвижной связи.

– X.1127, *Функциональные требования безопасности и функциональная архитектура для мер противодействия кражам мобильных телефонов*,котораяпосвящена функциональным требованиям безопасности и функциональной архитектуре механизмов противодействия кражам смартфонов, которые базируются на общих требованиях, сформулированных GSMA.

– Поправка 1 к X.1197, *Руководящие указания по критериям выбора криптографических алгоритмов для услуг IPTV и защиты контента*,гдесодержатсяобновленные Дополнения I и II, отражающие состояние дел в августе 2019 года, включая библиографические ссылки.

– X.1331, *Руководящие указания по безопасности для устройств домашней сети (HAN) в системах "умных" электросетей*,гдепредставлен анализ угроз для HAN в "умных" электросетях, требований к безопасности и функций безопасности. Поскольку роль и функции каждого устройства HAN различны, в ней приводятся требования к безопасности и функции безопасности в зависимости от устройств.

– X.1332, *Руководящие указания по безопасности услуг интеллектуального учета в "умных" электросетях*,гдесодержатся руководящие указания по безопасности услуг интеллектуального учета, которые позволяют поставщикам услуг реализовать соответствующие меры защиты для обеспечения безопасности предоставляемых ими услуг. Представлен анализ общей модели услуг интеллектуального учета в части уровня обслуживания. На базе общей модели в настоящей Рекомендации обсуждаются угрозы безопасности услуг интеллектуального учета и способы атак, направленных на эти услуги, а также требования по безопасности и средства обеспечения безопасности для снижения этих рисков. Кроме того, в настоящей Рекомендации представлены полезные стандарты безопасности, которые могут быть учтены при реализации поставщиком услуг возможностей обеспечения безопасности.

– X.1333, *Руководящие указания по безопасности для использования инструментов удаленного доступа в системах управления, подключенных к интернету*, где приведено полное описание безопасного использования инструментов удаленного доступа (RAT) для мониторинга, управления и технического обслуживания.

– X.1361, *Структура безопасности интернета вещей на основе модели с использованием шлюза*, где описывается структура безопасности интернета вещей (IoT) с использованием шлюзов безопасности. IoT – это глобальная инфраструктура для информационного общества, которая делает возможным предоставление перспективных услуг путем присоединения (физического и виртуального) вещей на основании существующих и развивающихся функционально совместимых информационно-коммуникационных технологий. В настоящей Рекомендации проводится анализ угроз и проблем безопасности в среде IoT и дается описание возможностей обеспечения безопасности, позволяющих снижать эти угрозы и решать проблемы безопасности. Представлена базовая методика определения тех возможностей обеспечения безопасности, которые необходимы для снижения угроз и решения проблем безопасности в сфере IoT.

– X.1362, *Простая процедура шифрования для среды интернета вещей (IoT)*,где определено шифрование с присоединенными данными для маскирования (EAMD) для устройств интернета вещей (IoT). Приведено описание EAMD и порядка предоставления набора услуг безопасности для трафика, в котором используется EAMD.

– X.1363, *Техническая структура обработки информации, позволяющей установить личность (PII), в среде интернета вещей (IoT)*,гдеопределена техническая структура обработки PII в среде IoT с одним или несколькими поставщиками услуг.

– X.1364, *Требования безопасности и структура безопасности узкополосного интернета вещей*,где определены угрозы и требования безопасности, характерные для развертывания NB-IoT, и таким образом создается структура мер безопасности, с помощью которой оператор может обеспечить защиту этой новой технологии.

– X.1365, *Методика обеспечения безопасности при использовании криптографии на основе идентичности в поддержку услуг интернета вещей (IoT) в сетях электросвязи*,гдесодержится методика обеспечения безопасности при использовании технологии открытых ключей IBC в поддержку услуг IoT в сетях электросвязи, включая механизмы управления определением идентичности, архитектуру управления ключами, операции управления ключами и аутентификацию.

– X.1366, *Схемы совокупной аутентификации сообщений для интернета вещей (IoT)*,гдеописаны две схемы аутентификации сообщений, одна из них – схема совокупной аутентификации сообщений (AMA) для среды IoT в качестве базового механизма. Другая – схема интерактивной совокупной аутентификации сообщений (IAMA) с интерактивным протоколом в упрощенном и безопасном режиме. Обе схемы совокупной аутентификации сообщений может применяться для обеспечения "аутентификации объекта (идентичности)", а также для обеспечения "аутентификации сообщений".

– X.1367, *Стандартный формат журналов регистрации ошибок в интернете вещей (IoT) для операций*, где описан стандартизованный формат журнала регистрации ошибок, который может быть помещен в полезную нагрузку протокола, например системный журнал регистрации (см. IETF RFC 5424), для использования в целях преобразования информации журнала регистрации ошибок, выданной граничным устройством, в стандартный формат журнала регистрации ошибок. В настоящей Рекомендации определена также таблица стандартизованных кодов ошибок для разрешения второй проблемы. В результате возможно комплексное управление инцидентами безопасности, происходящими в компьютерных сетях и сетях пограничных устройств IoT.

– X.1368, *Безопасное обновление микропрограммного или программного обеспечения устройств интернета вещей*, где определены: 1) базовые модели и процедуры, предназначенные для безопасного обновления микропрограммного или программного обеспечения (FW/SW) устройств интернета вещей (IoT); 2) требования и возможности для обновления FW IoT.

– X.1369, *Требования безопасности для платформы услуг IoT*, где определены требования безопасности для платформы услуг IoT. Проведена оценка угроз и проблем безопасности для платформы бизнес-услуг IoT и описаны меры обеспечения безопасности, которые могут смягчить угрозы и проблемы безопасности.

– X.1453, *Угрозы безопасности и требования безопасности для систем управления видео*, где проведен анализ угрозы безопасности для VMS (система управления видео) на основе серверной платформы, работающей в IP-сети, и определены требования безопасности для противодействия выявленным угрозам.

– X.1811, *Руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность*, где определены угрозы, которые квантовые вычисления создают для систем Международной подвижной электросвязи-2020 (IMT-2020), на основании оценки уровня безопасности используемых в настоящее время криптографических алгоритмов. В настоящей Рекомендации содержится краткий обзор алгоритмов, обеспечивающих квантовую безопасность, включая алгоритмы как симметричного, так и несимметричного типов, и приведены руководящие указания для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность.

– X.Suppl.26 Испр. 1, *МСЭ-T X.1111 − Добавление по функциональной архитектуре безопасности для услуг "умных" электросетей, использующих сети электросвязи.*

### g) Вопрос 7/17 − Безопасные прикладные услуги

В рамках Вопроса 7/17 разрабатываются Рекомендации, касающиеся требований безопасности для безопасных прикладных услуг, таких как дополнительные услуги и услуги в сфере финансовых технологий.

В течение рассматриваемого исследовательского периода в рамках Вопроса 7/17 разработаны девять новых Рекомендаций:

– X.1145, *Структура и требования безопасности для открытых возможностей услуг электросвязи*, где проводится анализ требований безопасности для открытых возможностей услуг электросвязи и определяется структура безопасности.

– X.1146, *Руководящие принципы обеспечения защиты для дополнительных услуг, предоставляемых операторами электросвязи*,гдепредставлены руководящие указания по защите секретности для дополнительных услуг, предоставляемых операторами электросвязи. В дополнение к анализу типовых сценариев услуг, угроз безопасности и методов атаки, в Рекомендация МСЭ-Т X.1146 представлены технические меры борьбы с угрозами и атаками. Это поможет операторам обеспечить безопасность дополнительных услуг и, наряду с этим, защитит преимущества пользователей.

– X.1147, *Требования и структура безопасности для аналитики больших данных в услугах мобильного интернета*,где будетпроведен анализ требований безопасности аналитики больших данных в услугах мобильного интернета и определена структура безопасности.

– X.1148, *Структура процесса деидентификации для поставщиков услуг электросвязи*,гдеописана структура процесса деидентификации, включая практические шаги, и на основе модели жизненного цикла данных и ролей участников определены модели публикации данных и этапы данных в процессе деидентификации для поставщиков услуг электросвязи.

– X.1149, *Структура безопасности открытой платформы для услуг в сфере финансовых технологий*,гдеописаны архитектура открытой платформы для услуг в сфере финансовых технологий (FinTech), угрозы и уязвимости открытой платформы, процедура использования открытого API для услуг FinTech. Также подробно представлены требования безопасности, относящиеся к открытой платформе услуг FinTech, как для финансовой компании, так для компании FinTech. В Дополнении к настоящей Рекомендации содержатся сценарии использования предлагаемой открытой платформы.

– X.1450, *Руководящие принципы для гибридной аутентификации и механизмов управления ключами в модели клиент-сервер*,гдеизложены руководящие принципы для гибридной аутентификации и механизмов управления ключами в модели клиент-сервер. Базовый механизм предполагает использование общих секретов и методов открытого ключа для аутентификации и обмена ключами. В настоящей Рекомендации рассматриваются сценарии обслуживания, угрозы безопасности и методы смягчения последствий соответствующих атак.

– X.1451, *Выявление рисков с целью оптимизации аутентификации*,гдеопределена функция выявления рисков в системе услуг ИКТ, которая действует в качестве препроцессора до вызова функции аутентификации. Оборудованная данной специальной функцией выявления рисков, система услуг ИКТ может осуществлять выбор механизмов аутентификации, адаптируясь к своим пользователям, и обеспечить ряд преимуществ, таких как: 1) повышение уровня удобства пользования; 2) увеличение пропускной способности и сокращение стоимости аутентификации пользователя на транзакцию; 3) снижение риска подделки идентичности пользователя.

– X.1452, *Руководящие указания в отношении услуг безопасности, предоставляемых операторами*, где проведена классификация вероятных сценариев использования услуг безопасности, предоставляемых операторами, и анализ конкретных требований к услугам безопасности, что обеспечивает руководящие указания для операторов по защите и совершенствованию своих услуг безопасности.

– X.1470, *Руководящие указания по безопасности веб-ориентированной онлайновой службы поддержки клиентов*, где проведен анализ угроз безопасности веб-ориентированной онлайновой службы поддержки клиентов в трех аспектах: безопасность сети, безопасность системы, безопасность услуг. Определены руководящие указания по безопасности веб-ориентированной онлайновой службы поддержки клиентов и соответствующие меры безопасности. Также предложены процедуры тестирования для проверки выполнения определенных требований безопасности с помощью соответствующих мер безопасности.

### h) Вопрос 8/17 − Безопасность облачных вычислений и инфраструктуры больших данных

В рамках Вопроса 8/17 разрабатываются Рекомендации, касающиеся угроз и требований безопасности для инфраструктуры облачных вычислений и больших данных.

В течение рассматриваемого исследовательского периода в рамках Вопроса 8/17 разработаны восемь новых Рекомендаций:

– X.1603, *Требования к безопасности данных для услуги мониторинга облачных вычислений*,гдепроводится анализ требований к безопасности данных для услуги мониторинга облачных вычислений, который включает требования к составу данных мониторинга, жизненный цикл данных мониторинга, требования к безопасности при сборе данных мониторинга и требования к безопасности при хранении данных мониторинга.

– X.1604, *Требования безопасности к сети как услуге (NaaS) в среде облачных вычислений*,гдеприведен анализ угроз и проблем безопасности сети как услуги (NaaS) в среде облачных вычислений и определены требования безопасности NaaS для приложения NaaS, платформы NaaS и связности NaaS на основе соответствующих типов облачных возможностей.

– X.1605, *Требования безопасности к открытой инфраструктуре как услуге (IaaS) в среде облачных вычислений*,гдесодержитсяописание требований безопасности к открытой IaaS в помощь поставщикам IaaS при повышении безопасности платформы IaaS на этапах планирования, создания и эксплуатации.

– X.1606, *Требования к безопасности прикладной среды связи как услуги*, гдеопределены угрозы безопасности и рекомендуются требования к безопасности прикладной среды связи как услуги (CaaS). В Рекомендации описаны сценарии и функции CaaS, содержащие возможности множественной связи. Определены также конкретные угрозы, обусловленные уникальными функциями CaaS, и рекомендуются надлежащие требования к безопасности CaaS.

– X.1643, *Требования безопасности и руководящие указания по безопасности контейнеров виртуализации в среде облачных вычислений*, где проведен анализ угроз и проблем безопасности для контейнеров виртуализации в среде облачных вычислений, а также определена эталонная структура, включающая руководящие указания по безопасности контейнеров виртуализации в облаке.

– X.1750, *Руководящие указания по безопасности больших данных как услуги для поставщиков услуг больших данных*,гдепроведен анализ проблем безопасности больших данных как услуги (BDaaS), определены функции и обязанности по обеспечению безопасности при предоставлении BDaaS, а также структура безопасности для инфраструктуры больших данных. Наряду с этим определены меры обеспечения безопасности, которые следует соблюдать в отношении услуг и компонентов, связанных с BDaaS.

– X.1751, *Руководящие указания по обеспечению безопасности при управлении жизненным циклом больших данных для операторов электросвязи*,гдесодержится анализ уязвимостей безопасности и определены руководящие указания для операторов электросвязи по обеспечению безопасности при управлении жизненным циклом больших данных. Представлены конкретные характеристики услуг электросвязи на основе больших данных и категории данных, анализируются уязвимости безопасности при управлении жизненным циклом больших данных и содержатся руководящие указания по безопасности для операторов электросвязи.

– X.1752, *Руководящие указания по безопасности для инфраструктуры и платформы больших данных*, где проведен анализ угроз и проблем безопасности, относящихся к инфраструктуре и платформе больших данных, а также определена эталонная структура для сопоставления руководящих указаний по безопасности и угроз для инфраструктуры и платформы больших данных.

– TR.XAASL, *Структура стандартизации безопасности для виртуализированных услуг,* документ для обсуждения вопросов разработки соображений, требований и структур стандартизации для виртуализированных услуг.

### i) Вопрос 9/17 − Телебиометрия (2017−2020 гг.)

В рамках Вопроса 9/17 разрабатываются Рекомендации по телебиометрии для аутентификации пользователей, использующих телебиометрию, и для защиты телебиометрической информации от несанкционированного доступа.

В течение рассматриваемого исследовательского периода в рамках Вопроса 9/17 разработаны три новые Рекомендации, одна пересмотренная Рекомендация и одно Исправление:

– X.1080.0 и Испр. 1 к X.1080.0, *Управление доступом для защиты телебиометрических данных*,гдеопределены способы защиты телебиометрической информации от несанкционированного доступа. В ней применяется ориентированный на услуги подход, при котором предоставляется лишь та информация, которая необходима для конкретной цели, то есть доступ к информации предоставляется не только на основе *права на информацию*, но и на основании *необходимости* в ней. Основным элементом настоящей Рекомендации является спецификация атрибута, содержащаяся в сертификате атрибутов или сертификате открытого ключа, которая подробно описывает круг привилегий того или иного объекта/субъекта для одного или нескольких типов услуг. Безопасность обеспечивается путем использования профиля синтаксиса криптографических сообщений (CMS). Этот профиль обеспечивает аутентификацию и целостность данных, а также при необходимости их конфиденциальность (шифрование). Профиль CMS призван служить средством поддержки безопасности во всевозможных телебиометрических спецификациях. Этот профиль предполагает наличие правильно развернутой инфраструктуры открытых ключей (PKI) и зависит от правильного развертывания такой инфраструктуры. Кроме того, применимость настоящей Рекомендации обусловлена развертыванием инфраструктуры управления привилегиями (PMI).

– X.1080.1 (пересмотренная), *Электронное здравоохранение и всемирная телемедицина – Общий протокол электросвязи*, гдеопределена структура других частей Рекомендаций МСЭ-T серии 1080.x в форме общей модели аспектов связи телебиометрии. Приведено базовое распределение идентификаторов объектов для однозначно идентифицируемых фрагментов информации в процессе передачи данных и определен общий протокол электросвязи. В Рекомендации представлен метод формального описания объектов и определен общий протокол, который обеспечивает взаимодействие между медицинским пунктом по месту жительства пациента и удаленным медицинским центром, имеющим в своем составе специалистов более высокой квалификации. Этот протокол следует использовать и расширять другими частями Рекомендаций МСЭ-Т серии X.1080.x.

– X.1093, *Телебиометрический контроль доступа с "умными" идентификационными картами*, гдеописана общая схема логического и/или физического контроля доступа с использованием биометрических данных на карте. Настоящая Рекомендация может применяться для недавно сформировавшейся области управления доступом, требующей безопасного физического, а также логического контроля доступа.

– X.1094, *Телебиометрическая аутентификация с использованием биосигналов*,гдеопределены новые методы надежной и строгой телебиометрической аутентификации c использованием биосигналов.

### j) Вопрос 10/17 − Архитектура и механизмы управления определением идентичности (2017−2020 гг.)/Архитектура и механизмы управления определением идентичности и телебиометрии (2021 г. −)

В рамках Вопроса 10/17 разрабатываются Рекомендации по вопросам управления определением идентичности, включая структуры аутентификации. В январе 2021 года Вопросу 10/17 была передана работа по телебиометрии, ранее проводимая по Вопросу 9/17.

В течение рассматриваемого исследовательского периода в рамках Вопроса 10/17 разработаны пять новых Рекомендаций, две пересмотренные Рекомендации и одно новое Добавление:

– X.1080.2, *Протокол биология-машина (B2M)*, где определен общий протокол для обмена биометрической информацией, поступающей от оборудования пациента в оборудование медицинского специалиста, с тем чтобы медицинский центр мог осуществлять удаленный мониторинг пациента и получать информацию от этого пациента.

– X.1252 (пересмотренная), *Базовые термины и определения в области управления определением идентичности*, где приведены определения основных терминов, используемых в области управления определением идентичности (IdM). Эти термины взяты из многих источников, однако считается, что все эти источники являются общеупотребительными в работе в области IdM. Данная Рекомендация не рассчитана на то, чтобы стать большим сборником терминов, относящихся к IdM. Напротив, определенные в Рекомендации термины ограничены теми терминами, которые, как предполагается, составляют базовый перечень наиболее важных и общеупотребительных терминов, касающихся IdM. В настоящую Рекомендацию включено Приложение А, в котором приводятся соображения, лежащие в основе некоторых из этих основных терминов.

− X.1254 (пересмотренная), *Структура гарантии аутентификации объекта*, гдеопределены три уровня гарантии аутентификации объекта (AAL), а также критерии и угрозы для каждого из этих трех уровней.

Кроме того:

• определена структура управления AAL;

• на основе оценки риска приведены руководящие указания по методам контроля, которые должны использоваться в целях смягчения угроз аутентификации;

• приведено руководство по картированию этих трех AAL в другие схемы гарантии аутентификации; и

• приведено руководство по обмену результатами аутентификации, основанными на трех AAL.

− X.1276, *Протокол и метаданные поэтапной аутентификации, версия 1.0*, гдеобеспечены простые архитектурные модели для повышения доверия, демонстрирующие использование повышения доверия в современной архитектуре контроля доступа; описаны общие наборы метаданных, элементы механизмов и протоколов для обмена информацией о повышении доверия; обеспечено содействие использованию элементов повышения доверия для упрощения стандартизации в рамках большого числа технологий и подходов, которые используются в настоящее время для снижения рисков, связанных с регистрационными данными и аутентификацией.

– X.1277, *Структура универсальной аутентификации*,гдеописана структура универсальной аутентификации (UAF) FIDO, которая обеспечивает возможность прозрачного использования онлайновыми услугами и веб-сайтами, в открытом интернете или в рамках предприятия, собственных функций безопасности вычислительных устройств конечных пользователей для двухфакторной аутентификации пользователей и сокращения числа проблем, связанных с созданием и хранением в памяти большого числа онлайновых учетных данных.

– X.1278, *Протокол клиент-аутентификатор/универсальная двухфакторная схема*,гдеописан протокол прикладного уровня для связи между внешним аутентификатором и другим клиентом/другой платформой, а также увязка этого прикладного протокола и разнообразных протоколов транспортирования с использованием различных физических носителей.

– X.1279, *Система расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения*,гдепредставлена архитектурная основа системы расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения. В настоящей Рекомендации проведен анализ угроз для традиционных решений телебиометрической аутентификации и представлены архитектурная основа системы и последовательность операций аутентификации, а также рассмотрены вопросы безопасности расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения.

– X.Suppl.35, *МСЭ-T X.1254 − Добавление, касающееся случаев использования структуры гарантии аутентификации объекта (EAA)*, гдесодержатся три сценария применения структуры гарантии аутентификации объекта при внедрении систем безопасности, включая подробные соображения безопасности при оценке рисков, выборе надлежащего уровня гарантии и выборе технологий аутентификации.

Кроме того, ИК17 на своем электронном пленарном заседании 29 мая 2020 года приняла решение присвоить номер X.1261 Рекомендации МСЭ-T D.1140 "*Политическая основа, включая принципы для инфраструктуры цифровой идентичности*", для того чтобы эта Рекомендация имела двойную нумерацию как Рекомендация МСЭ‑Т серии D и Рекомендация МСЭ-T серии X по управлению определением идентичности.

### k) Вопрос 11/17 − Общие технологии (Справочник, инфраструктура открытых ключей (PKI), инфраструктура управления привилегиями (PMI), абстрактная синтаксическая нотация № 1 (ASN.1), идентификаторы объектов (OID)) для поддержки безопасных приложений (2017−2020 гг.)/Общие технологии (например, Справочник, PKI, формальные языки, идентификаторы объекта) для поддержки безопасных приложений (2021 г. −)

В рамках Вопроса 11/17 разрабатываются Рекомендации по справочным службам и системам, включая сертификаты открытых ключей/атрибутов в Рекомендациях серии X.500. В рамках Вопроса 11/17 осуществляется ведение Рекомендаций по ASN.1 и дальнейшая разработка Рекомендаций по OID – всемирно известной схеме идентификации, основанной на иерархических органах регистрации, получившей название "дерево идентификаторов объектов". В январе 2021 года Вопросу 11/17 была передана работа по языкам, ранее проводимая по Вопросу 12/17.

В течение рассматриваемого исследовательского периода в рамках Вопроса 11/17 разработаны пять новых Рекомендаций, 20 пересмотренных Рекомендаций, одна Поправка и 14 Технических исправлений (X.680 Испр. 1, X.680 Испр. 2, X.680 Попр. 1, X.680 Испр. 3, X.681 Испр. 1, X.682 Испр. 1, X.682 Испр. 2, X.683 Испр. 1, X.693 Испр. 1, X.694 Испр. 1, X.696 Испр. 1, X.696 Испр. 2, X.696 Испр. 3, X.893 Испр. 1, X.894 Испр. 1) к Рекомендациям серий X.500, X.680 и X.690, а также одно Добавление и один новый Технический отчет:

− X.500 (пересмотренная), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Обзор понятий, моделей и услуг*, знакомит с понятиями Справочника и DIB (информационная база Справочника), а также содержит обзор услуг и возможностей, которые они предоставляют.

− X.501 (пересмотренная), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Модели*, предлагает ряд различных моделей Справочника в качестве основы для других Рекомендаций МСЭ-Т серии X.500. Этими моделями являются общая (функциональная) модель, модель административных полномочий, обобщенные информационные модели Справочника, дающие пользователю Справочника и административному пользователю представление об информации Справочника, обобщенных моделях системного агента Справочника (DSA) и информационных моделях DSA, а также об эксплуатационной структуре и о модели обеспечения безопасности.

– Попр. 1 к X.501, *Информационные технологии – Взаимосвязь открытых систем – Справочник: Модели*, обновление раздела 9.2 и Приложения A.

− X.509 (пересмотренная), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов*, содержит определение структур для инфраструктуры открытых ключей (PKI) и инфраструктуры управления привилегиями (PMI). В ней вводится базовое понятие асимметричных методов шифрования. В ней определяются следующие типы данных: сертификат открытых ключей, сертификат атрибутов, список аннулированных сертификатов (CRL) и список аннулированных сертификатов атрибутов (ACRL). В ней содержится также определение некоторых сертификатов и расширений CRL и определяется информация схемы справочника, позволяющая хранить в справочнике данные, относящиеся к PKI и PMI. Кроме того, в ней определяются типы объектов, такие как орган по сертификации (CA), орган по присвоению атрибутов (AA), использующая сторона, верификатор привилегий, брокер доверия и точка доверия. В ней определяются принципы для проверки сертификата, путь проверки, стратегия в отношении сертификатов и т. д. Она включает спецификацию для списков проверки авторизации, которые позволяют осуществить быструю проверку и ввести ограничения на связь. Она включает также протоколы, необходимые для ведения списков проверки авторизации, а также протокол для получения доступа к брокеру доверия.

– Испр. 1 к X.509, *Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов*, исправление ошибок в разделе 6.2.2 и Приложении B.

− X.510, *Информационные технологии – Взаимосвязь открытых систем – Справочник:* *Спецификация протокола для безопасных операций*, где определен общий протокол, называемый протоколом оболочки, который обеспечивает кибербезопасность для протоколов, предназначенных для защиты протокола оболочки, путем обеспечения аутентификации, целостности данных и, при необходимости, конфиденциальности (шифрования). Протокол оболочки позволяет обеспечивать кибербезопасность независимо от защищенных протоколов, что означает, что безопасность может быть усилена без ущерба для спецификации защищенного протокола.

− X.511 (пересмотренная), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Определение абстрактной службы*, где определены в абстрактной форме обеспечиваемые справочником услуги, видимые внешнему пользователю, в том числе операции привязывания и отвязывания, чтения, поиска, модификации и поддержки политики в отношении паролей и поддержки взаимодействия с LDAP. В ней определяются также ошибки.

− X.518 (пересмотренная), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Процедуры распределенных операций*, где определены процедуры, с помощью которых распределенные компоненты справочника, состоящие из сочетания серверов системных агентов справочника (DSA) и облегченного протокола доступа к справочникам (LDAP), взаимодействуют для того, чтобы предоставить своим пользователям согласованную услугу, независящую от точки доступа. В ней также описаны процедуры преобразования протокола между протоколом доступа к справочнику/системным протоколом справочника (DAP/DSP) и протоколом LDAP.

− X.519 (пересмотренная), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Спецификации протоколов*, где определен протокол доступа к справочнику, системный протокол справочника, протокол теневого копирования информации справочника и протокол управления операционным связыванием справочника, которые выполняют абстрактные услуги, определенные в Рекомендации МСЭ-Т X.501 | ИСО/МЭК 9594-2, Рекомендации МСЭ-Т X.511 | ИСО/МЭК 9594-3, Рекомендации МСЭ-Т X.518 | ИСО/МЭК 9594-4 и Рекомендации МСЭ-Т X.525 | ИСО/МЭК 9594-9. В нее включены спецификации для поддержки базовых протоколов в целях снижения зависимости от внешних спецификаций. Эти протоколы могут кодироваться с использованием всех стандартных правил кодирования ASN.1.

− X.520 (пересмотренная), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Избранные типы атрибутов*, где определены несколько типов атрибутов и правил сопоставления, которые могут оказаться полезными в ряде приложений справочника. Одним конкретным случаем применения большого числа определенных здесь атрибутов является формирование имен, в частности для классов объектов, определенных в Рекомендации МСЭ-Т X.521 | ИСО/МЭК 9594-7. Другие типы атрибутов, называемые атрибутами уведомления, обеспечивают диагностическую информацию. В этой Рекомендации | Международном стандарте определяются типы контекста, которые предоставляют характеристики, связанные со значениями атрибутов. В нее также включены определения синтаксиса LDAP, относящиеся к типам атрибутов и правилам сопоставления.

− X.521 (пересмотренная), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Избранные объектные классы*, где определено некоторое количество избранных объектных классов и форм имени, которые могут оказаться полезными для целого ряда приложений Справочника. Определение объектного класса устанавливает типы атрибутов, которые относятся к объектам данного класса. Определение формы имени устанавливает атрибуты, которые должны использоваться при задании названий для объектов данного класса.

− X.525 (пересмотренная), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Копирование*, где определена служба зеркального копирования, которую системные агенты справочника (DSA) могут использовать для копирования информации Справочника. Эта служба позволяет нескольким DSA копировать информацию Справочника для улучшения обслуживания пользователей Справочника и обеспечивает автоматическое обновление этой информации.

– X.676, *Структура разрешения на базе идентификатора объекта для сгруппированных услуг IoT*,гдеопределена структура разрешения на базе идентификатора объекта (OID) для идентификации различных услуг в среде IoT. OID – это идентификатор для наименования объекта с использованием иерархически присваиваемого пространства имен. В интернете вещей (IoT) тысячи услуг IoT, основанных на неоднородных ресурсах, будут предоставляться как комбинация различных услуг. Для повышения эффективности потребуются различные технологии, такие как привязка услуг, динамические услуги или часто переключаемые услуги, а также разрешение и идентификация сгруппированных услуг. В данной Рекомендации изложены понятия сгруппированных услуг IoT, соображения, архитектуры и процедуры для структуры разрешения на основе OID для сгруппированных услуг IoT.

– X.677, *Механизм идентификации для беспилотных летательных аппаратов с использованием идентификаторов объектов*, где проведен анализ требований к управлению полным жизненным циклом и распознаванию эксплуатационной идентичности беспилотных летательных аппаратов (БПЛА) с учетом соображений безопасности, а также определен механизм идентификации БПЛА с использованием идентификаторов объектов (OID), включая подробные спецификации правил присвоения и процедур регистрации для OID, используемых для БПЛА.

– X.680 (пересмотренная, а также Попр. 1 и Испр. 1–3 к ней, выпущенные до пересмотра), *Информационная технология – Абстрактная синтаксическая нотация № 1 (ASN.1): Спецификация базовой нотации,* где представлена нотация, называемая абстрактной синтаксической нотацией версии один (ASN.1) для определения синтаксиса информационных данных. Определен ряд простых типов данных и задана нотация для ссылок на эти типы данных и для указания значений этих типов.

– X.681 (пересмотренная, а также Испр. 1 к ней, выпущенное до пересмотра), *Информационная технология – Абстрактная синтаксическая нотация № 1 (ASN.1): Спецификация информационных объектов*, где представлена нотация ASN.1, которая позволяет определять классы информационных объектов, отдельные информационные объекты и их наборы, а также заданные имена ссылок. Класс информационного объекта определяет форму концептуальной таблицы (набор информационных объектов), в которой один столбец соответствует каждому полю в классе информационного объекта, а каждая заполненная строка определяет информационный объект.

– X.682 (пересмотренная, а также Испр. 2 к ней, выпущенное до пересмотра), *Информационная технология – Абстрактная синтаксическая нотация № 1 (ASN.1): Спецификация ограничений*, где представлена нотация ASN.1 для общего случая спецификации ограничений и исключений, с помощью которой могут быть ограничены значения данных структурированного типа. Эта нотация также предусматривает сигнализацию при каком-либо нарушении ограничений.

– X.683 (пересмотренная, а также Испр. 1 к ней, выпущенное до пересмотра), *Информационная технология – Абстрактная синтаксическая нотация № 1 (ASN.1): Параметризация спецификаций ASN.1*, где определены положения, касающиеся параметризованных справочных имен и параметризованных присвоений для типов данных, которые помогают разработчикам в составлении спецификаций в тех случаях, когда на некоторых этапах разработки какие-либо аспекты остаются неопределенными до более позднего этапа, когда вырабатывается полное определение абстрактного синтаксиса.

– X.690 (пересмотренная), *Информационная технология – Правила кодирования ASN.1: Спецификация базовых правил кодирования (BER), канонических правил кодирования (CER) и отличительных правил кодирования (DER)*, где описан набор базовых правил кодирования (BER), которые могут применяться к значениям типов, определяемых с использованием нотации ASN.1. Применение этих правил кодирования позволяет получить синтаксис передачи для таких значений. Спецификация указанных правил кодирования подразумевает, что они используются также для декодирования. В настоящей Рекомендации | Международном стандарте приведен также набор отличительных правил кодирования (DER) и набор канонических правил кодирования (CER), которые налагают ограничения на базовые правила кодирования (BER). Ключевым различием между ними является то, что правила DER используют форматы кодирования определенной длины, тогда как правила CER используют форматы неопределенной длины. Правила DER более подходят для малых кодируемых значений, а правила CER – для больших значений. Спецификация указанных правил кодирования подразумевает, что они используются также для декодирования.

– X.691 (пересмотренная), *Информационная технология – Правила кодирования ASN.1: Спецификация правил пакетного кодирования (PER)*, где описан набор правил кодирования, который возможно применять к значениям любых типов ASN.1 в целях получения гораздо более компактного представления, чем это возможно, при помощи базовых правил кодирования и их производных (описанных в Рекомендации МСЭ-T X.690 | ИСО/МЭК 8825‑1).

– X.692 (пересмотренная), *Информационная технология – Правила кодирования ASN.1: Спецификация нотации управления кодированием (ECN)*, где определена нотация управления кодированием (ECN), используемая для определения кодирований (типов ASN.1), которые отличаются от представленных в стандартизованных правилах кодирования, таких как базовые правила кодирования (BER) и правила пакетного кодирования (PER).

– X.693 (пересмотренная, а также Испр. 1 к ней, выпущенное до пересмотра), *Информационная технология – Правила кодирования ASN.1: Правила кодирования языка XML (XER)*, где определены правила кодирования значений типов ASN.1 с использованием расширяемого языка разметки (XML).

– X.694 (пересмотренная, а также Испр. 1 к ней, выпущенное до пересмотра), *Информационные технологии – Правила кодирования ASN.1: Отображение определений схемы языка XML консорциума W3C в системе обозначений ASN.1*, где определены правила отображения схемы XSD (схемы, соответствующей спецификации схемы языка XML консорциума W3C) в схему абстрактной синтаксической нотацией версии один (ASN.1), чтобы использовать такие правила кодирования ASN.1, как базовые правила кодирования (BER), отличительные правила кодирования (DER), правила пакетного кодирования (PER) и правила кодирования языка XML (XER) для передачи информации, определяемой схемой XSD.

– X.695 (пересмотренная), *Информационная технология – Правила кодирования ASN.1: Регистрация и применение инструкций по кодированию PER*, где определены правила применения инструкций по кодированию PER с использованием либо префиксов типов, либо секции управления кодированием. Инструкции по кодированию являются средством модификации кодировок типов ASN.1 для какого-либо определенного правила кодирования (в данном случае PER). Они могут быть либо вставлены в спецификацию ASN.1 в квадратных скобках (как теги в базовых правилах кодирования, BER) непосредственно перед типом, к которому они относятся (префиксы типов), либо собраны вместе в конце модуля ASN.1 (секции управления кодированием).

– X.696 (пересмотренная, а также Испр. 1–3 к ней, выпущенные до пересмотра), *Информационные технологии − Правила кодирования ASN.1 – Спецификация правил кодирования по октетам (OER)*, где описаны два набора правил двоичного кодирования, которые могут применяться к значениям любых типов ASN.1, используя при этом меньший объем ресурсов обработки информации по сравнению с базовыми правилами кодирования и их производными (описанными в Рекомендации МСЭ-T X.690 | ИСО/МЭК 8825-1), а также правилами пакетного кодирования (описанными в Рекомендации МСЭ-T X.691 | ИСО/МЭК 8825-2).

– X.697, *Информационная технология – Правила кодирования ASN.1: Спецификация правил кодирования нотации объектов JavaScript (JER),* где определен набор правил кодирования нотации объектов JavaScript (JER), которые могут использоваться для получения синтаксиса передачи для значений, определенных в Рекомендации МСЭ-T X.680 | ISO/IEC 8824-1, в Рекомендации МСЭ-T X.681 | ISO/IEC 8824-2, в Рекомендации МСЭ-T X.682 | ISO/IEC 8824‑3 и в Рекомендации МСЭ-T X.683 | ISO/IEC 8824-4. Спецификация указанных правил кодирования подразумевает, что они используются также для декодирования.

– Испр. 1 к X.893 *Информационные технологии – Общие приложения ASN.1: Безопасность быстрого информационного набора,* где введены поправки к информационным приложениям и Библиографии, которые заключаются в удалении ссылок на устаревший алгоритм тройного DES.

– X.894, *Информационные технологии – Общие приложения ASN.1 – Синтаксис криптографических сообщений*,гдепредставлены модули абстрактной синтаксической нотации версии один (ASN.1) для использования криптографического синтаксиса в Рекомендациях МСЭ-Т. Синтаксис криптографических сообщений (CMS) позволяет оказывать услуги обеспечения целостности данных, конфиденциальности, аутентичности источника и предотвращения отказа от авторства, необходимые для обмена надежной информацией и для строгой аутентификации. Также сформирован набор методов управления криптографическими ключами для поддержки гибких механизмов создания ключей, таких как конструктивное управление ключами, согласование ключей, обмен ключами и шифрование на основе паролей. Эти методы могут использоваться для предотвращения мошенничества и защиты информации, позволяющей установить личность, и другой критичной информации. Эта Рекомендация | Международный стандарт поддерживает методы цифровой подписи, шифрования и шифрования с подписью (signcryption) на основе технологии открытого ключа, описанной в серии МСЭ‑T X.500 | Стандарте ИСО/МЭК 9594, состоящем из нескольких частей. Поддерживаются все стандартные правила кодирования для ASN.1.

– Z.161 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Основной язык TTCN-3*, которая предназначена для спецификации комплектов тестов, не зависимых от платформ, методов тестирования, уровней протоколов и протоколов. TTCN-3 может использоваться для спецификации всех типов тестов реагирующих систем через различные порты связи.

– Z.161.2 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: TTCN-3 Расширения для языка TTCN-3: Конфигурация и поддержка развертывания*, где определена конфигурация и развертывание поддерживающего пакета TTCN-3. TTCN-3 может использоваться для спецификации всех типов тестов реагирующих систем через различные порты связи.

– Z.161.3 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Усовершенствованная параметризация*, где определен пакет усовершенствованной параметризации TTCN-3. TTCN-3 может использоваться для спецификации всех типов тестов реагирующих систем через различные порты связи.

– Z.161.4 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Типы поведения*, где определен пакет типов поведения TTCN‑3. TTCN-3 может использоваться для спецификации всех типов тестов реагирующих систем через различные порты связи.

– Z.161.7 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Объектно-ориентированные свойства*, где определена поддержка объектно-ориентированных свойств в TTCN-3. TTCN-3 может использоваться для спецификации всех типов тестов реагирующих систем через различные порты связи.

– Z.167 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Использование ASN.1 вместе с TTCN-3*, где определен нормативный способ использования Абстрактной синтаксической нотации версии 1, которая определена в Рекомендациях МСЭ-T X.680, МСЭ-T X.681, МСЭ-T X.682 и МСЭ-T X.683, вместе с TTCN-3.

– Z.168 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Преобразование из CORBA IDL TTCN-3*, где определены правила отображения языка описания интерфейса (IDL) обобщенной архитектуры посредника объектных запросов (CORBA) в язык TTCN-3 (определенный в Рекомендации МСЭ Т Z.161), для того чтобы обеспечить возможность тестирования систем на базе CORBA. Принципы отображения CORBA IDL в TTCN-3 возможно также использовать для отображения языков спецификаций интерфейса других технологий на основе объектов/компонентов.

– Z.169 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Преобразование из определения данных XML TTCN-3*, где определены правила отображения схемы Консорциума World Wide Web (W3C) в нотацию тестирования и управления тестированием версии 3 (TTCN-3), для того чтобы обеспечить возможность тестирования базирующихся на XML систем, интерфейсов и протоколов.

– Z.171 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Использование JSON с TTCN-3*, где описаны правила определения схем для структур данных JSON в TTCN-3, для того чтобы обеспечить возможность тестирования систем, интерфейсов и протоколов на базе JSON, а также правила преобразования между TTCN-3 и JSON, для того чтобы обеспечить возможность обмена данными TTCN-3 в формате JSON между различными системами.

– X.Suppl.31, *МСЭ-T X.660 − Руководящие указания по использованию идентификаторов объектов для интернета вещей*, где содержатся руководящие указания по использованию идентификаторов объектов (OID) для интернета вещей (IoT). Сюда относятся руководящие указания по созданию структуры OID, реализации систем разрешения, а также установлению процедур управления на базе существующих Рекомендаций МСЭ-Т и международных стандартов.

– XSTP-OID-ORS, *Система разрешения для OID: Проблемы, требования и возможные решения*, где определены проблемы, требования и возможныерешения в отношении разрешения для OID. Проблемы включают качество работы на локальном уровне и глобальное разрешение для отсутствующих поддеревьев OID. Также обсуждаются технические требования к возможным решениям. Наконец, представлены возможные технические решения, руководства по администрированию и эксплуатации.

– Z.Imp100 (пересмотренное), *Руководство пользователя Рекомендаций по языку спецификации и описания – Версия 4.0.1*, в котором содержится подборка сообщенных дефектов и проблем поддержания вместе с решениями по их устранению для Рекомендаций МСЭ-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 и Z.119, относящихся к языку спецификации и описания*.*

### l) Вопрос 12/17 − Формальные языки для программного обеспечения систем электросвязи и тестирования (2017−2020 гг.)

В рамках Вопроса 12/17 разрабатываются Рекомендации, касающиеся формальных языков (например, SDL, MSC, URN), для определения требований, архитектуры и поведения систем электросвязи: языки требований, языки спецификации и реализации. В рамках Вопроса 12/17 также ведется разработка Рекомендаций по языкам тестирования (например, TTCN-3) как средству обеспечения возможности функциональной совместимости и соответствия.

В данном исследовательском периоде в рамках Вопроса 12/17 были разработаны три новые Рекомендации, 44 пересмотренные Рекомендации и два пересмотренных руководства пользователя:

− Z.100 (пересмотренная), *Язык спецификации и описания: Обзор SDL-2010*, где представлен язык спецификации и описания, предназначенный для однозначной спецификации и описания систем электросвязи.

− Z.100, Приложение F1 (пересмотренное), *Формальное определение SDL-2010: Общий обзор*, где содержится обоснование, приведен обзор структуры формальной семантики, а также содержится введение в формализм машины абстрактных состояний (ASM), который используется для определения семантики SDL-2010.

− Z.100, Приложение F2 (пересмотренное), *Формальное определение SDL-2010: Статическая семантика*, где содержится описание ограничений статической семантики и преобразований, определенные в разделах "Модель" Рекомендаций МСЭ-T Z.101, Z.102, Z.103, Z.104, Z.105 и Z.107, которые посредством ссылки включены в Рекомендацию МСЭ-T Z.100.

− Z.100 Приложение F3 (пересмотренное), *Формальное определение SDL-2010: Динамическая семантика*, где содержится определение динамичной семантики SDL‑2010.

− Z.101 (пересмотренная), *Язык спецификации и описания − Основной SDL-2010*, где содержится определение основных свойств языка спецификации и описания. Язык, определенный в этом документе, охватывает важнейшие свойства языка, который далее определяется в других Рекомендациях МСЭ-Т серии Z.100.

− Z.102 (пересмотренная), *Язык спецификации и описания − Комплексный SDL-2010*, где содержится определение полного набора свойств языка спецификации и описания. Язык, определенный в этом документе, охватывает свойства языка, не входящие в основной SDL‑‎‎2010, описанный в Рекомендации МСЭ-T Z.101. Эти свойства обеспечивают полный охват абстрактной грамматики этого языка, за исключением свойств некоторых данных, приведенных в Рекомендации МСЭ-T Z.104 (и Рекомендации МСЭ-T Z.107 для объектно-ориентированных данных).

− Z.103 (пересмотренная), *Язык спецификации и описания – Краткие нотации и аннотации в SDL-2010*, где содержится определение свойств краткой нотации и аннотации языка спецификации и описания. Язык, определенный в этом документе, охватывает свойства языка, не входящие в основной SDL-‎‎2010, описанный в Рекомендации МСЭ-Т Z.101, или в комплексный SDL 2010, описанный в Рекомендации МСЭ-Т Z.102. Свойства, определенные в настоящей Рекомендации, либо не имеют своей собственной абстрактной грамматики и преобразуются для соответствия конкретной грамматике, определенной в Рекомендациях МСЭ-Т Z.101, МСЭ-Т Z.102 и МСЭ-Т Z.104 (и Рекомендации МСЭ-T Z.107 для объектно-ориентированных данных), либо являются аннотациями без формального значения.

− Z.104 (пересмотренная), *Язык спецификации и описания − Язык данных и действий в SDL‑2010*, где содержится определение свойств данных языка спецификации и описания, с тем чтобы определения и выражения данных были правильно сформулированы. Определенный в данном документе язык частично дублирует свойства языка, включенные в основной SDL-2010, описанный в Рекомендации МСЭ-Т Z.101, и используемые в комплексном SDL-‎‎2010, описанном в Рекомендации МСЭ-T Z.102, а также свойства Рекомендации МСЭ-T Z.103.

− Z.105 (пересмотренная), *Язык спецификации и описания – Сочетание SDL-2010 с модулями ASN.1*, где определено, каким образом модули абстрактной синтаксической нотации версии 1 (ASN.1) могут быть использованы в сочетании с языком спецификации и описания 2010 года (SDL‑2010). Этот текст заменяет Рекомендацию МСЭ-Т Z.105 (2003) в целях согласования с Рекомендациями МСЭ-Т Z.100, МСЭ-Т Z.101, МСЭ-Т Z.102, МСЭ-Т Z.103, МСЭ-Т Z.104, МСЭ-Т Z.106 и МСЭ-Т Z.107 для SDL-2010. Рекомендация МСЭ-Т Z.105 (2003) заменила семантические отображения от ASN.1 в SDL-2000, определенные в Рекомендации МСЭ-Т Z.105 (1999).

− Z.106 (пересмотренная), *Язык спецификации и описания – Общий формат обмена для SDL‑2010*, где содержится определение общего формата обмена для языка спецификации и описания (SDL-CIF). Формат SDL-CIF предназначен для обмена графическими спецификациями SDL-2010 (SDL-GR), выполненными с помощью различных средств, которые не используют один и тот же формат хранения данных. Настоящая Рекомендация вводит два дополнительных уровня формата SDL CIF. Определяются два дополнительных уровня соответствия, один на более свободном уровне SDL PR и второй, включающий графическую информацию.

− Z.107 (пересмотренная), *Язык спецификации и описания – Объектно-ориентированные данные в SDL-2010*, где определены объектно-ориентированные свойства данных языка спецификации и описания на основе определений данных и выражений, приведенных в Рекомендации МСЭ-Т Z.104. Определенный в данной Рекомендации язык частично дублирует свойства языка, включенные в основной SDL-2010, описанный в Рекомендации МСЭ-Т Z.101, и используемые в комплексном SDL-‎‎2010, описанном в Рекомендации МСЭ-T Z.102, а также свойства Рекомендаций МСЭ-T Z.103 и МСЭ-Т Z.104.

− Z.151 (пересмотренная), *Нотация требований пользователя (URN) – Определение языка*, где содержится определение нотации требований пользователя (URN), предназначенной для выявления, анализа, описания и валидации требований. URN сочетает понятия и нотации моделирования для целей (в основном для нефункциональных требований и атрибутов качества) и сценариев (в основном для эксплуатационных требований, функциональных требований, а также из соображений функциональных характеристик и архитектуры). Поднотация цели получила название языка требований, ориентированных на цель (GRL), а поднотация сценария – отображения сценариев использования (UCM).

− Z.161 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Основной язык TTCN-3*, где содержится определение нотации для тестирования и управления тестированием версии 3 (TTCN-3), предназначенной для спецификации наборов тестов, не зависимых от платформ, методов тестирования, уровней протоколов и протоколов. TTCN-3 может использоваться для спецификации всех типов тестов реагирующих систем через различные порты связи. Типичными областями применения являются тестирование протоколов (включая протоколы подвижной связи и протокол Интернет), тестирование услуг (включая дополнительные услуги), тестирование модулей, тестирование платформ на базе общей архитектуры брокера объектных запросов (CORBA) и тестирование интерфейсов прикладного программирования (API).

− Z.161.1 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Поддержка интерфейсов с постоянными сигналами*, где определен пакет TTCN-3 "поддержка постоянных сигналов". TTCN-3 может использоваться для спецификации всех типов тестов реагирующих систем через различные порты связи. Типичными областями применения являются тестирование протоколов (включая протоколы подвижной связи и протокол Интернет), тестирование услуг (включая дополнительные услуги), тестирование модулей, тестирование платформ на базе CORBA, тестирование интерфейсов API и т. д. Применение TTCN-3 не ограничивается тестированием на соответствие; этот язык может использоваться для многих других видов тестирования, в том числе для тестирования функциональной совместимости, устойчивости, регрессии, систем и интеграции. Спецификация наборов тестов для протоколов физического уровня выходит за рамки данного документа.

− Z.161.2 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Конфигурация и поддержка развертывания*, где определены конфигурация и развертывание поддерживающего пакета TTCN-3.

− Z.161.3 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Усовершенствованная параметризация*, где определен пакет усовершенствованной параметризации TTCN-3.

− Z.161.4 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Типы поведения*, где определен пакет типов поведения TTCN-3.

− Z.161.6 (новая и пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Сопоставление сигнатур*, где определена поддержка усовершенствованного согласования нотации для тестирования и управления тестированием версии 3 (TTCN-3).

− Z.161.7 (новая и пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Объектно-ориентированные свойства*,гдеопределена поддержка объектно-ориентированных свойств в нотации тестирования и управления тестированием версии 3 (TTCN-3).

− Z.164 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Операционная семантика TTCN-3*, где определена операционная семантика TTCN-3 (Нотация для тестирования и управления тестированием версии 3). Операционная семантика необходима для однозначной интерпретации спецификаций, разработанных с использованием TTCN-3. Данная Рекомендация опирается на базовый язык TTCN-3, который определен в Рекомендации МСЭ-Т Z.161. В этом пересмотре Рекомендации содержатся поправки, разъяснения, исправления и редакционные правки.

− Z.165 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Интерфейс времени выполнения TTCN-3 (TRI)*, где содержится спецификация интерфейса времени выполнения для реализаций тестовой системы согласно TTCN-3 (нотация тестирования и управления тестированием версии 3). Интерфейс времени выполнения с использованием TTCN-3 обеспечивает рекомендуемую адаптацию для синхронизации и связи тестовой системы с конкретной платформой обработки и с тестируемой системой соответственно. В настоящей Рекомендации интерфейс определяется как набор операций, не зависимых от целевого языка.

Интерфейс определен как совместимый с Рекомендацией МСЭ-Т Z.161. Для полного описания TRI в настоящей Рекомендации используется язык описания интерфейса (IDL) обобщенной архитектуры посредника объектных запросов (CORBA). В разделах 6, 7 и 8 стандарта ETSI ES 201 873-5 V4.8.1 приведено описание отображения языка абстрактной спецификации в целевые языки Java и ANSI-C. В Приложении A стандарта ETSI ES 201 873‑5 V4.8.1 содержится резюме спецификации интерфейса на базе IDL.

В этом пересмотре Рекомендации содержатся поправки, разъяснения, исправления и редакционные правки.

− Z.166 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Интерфейс управления TTCN-3 (TCI)*, где содержится описание интерфейсов управления для реализаций тестовой системы согласно нотации для тестирования и управления тестированием версии 3 (TTCN-3). Интерфейсы управления TTCN-3 (TCI) обеспечивают стандартизованную адаптацию администрирования, обработки тестового компонента и кодирования/декодирования тестовой системы к отдельной тестовой платформе. В этой Рекомендации интерфейсы определяются как набор операций, независимых от целевого языка.

Интерфейсы определяются как совместимые со стандартами TTCN-3 (см. раздел 2 ETSI ES 201 873-6 V4.11.1). Для полного определения интерфейса TCI в описании интерфейса используется язык описания интерфейса (IDL) общей архитектуры брокера объектных запросов (CORBA). В разделах 8, 9 и 9.7 стандарта ETSI ES 201 873-6 V4.11.1 приведено описание отображений языка данной абстрактной спецификации в целевые языки Java и ANSI C.

В этом пересмотре Рекомендации содержатся поправки, разъяснения, исправления и редакционные правки.

− Z.167 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Преобразование ASN.1 в TTCN-3*, где содержится описание нормативного способа использования ASN.1, как определено в Рекомендациях МСЭ-T X.680, МСЭ-T X.681, МСЭ-T X.682 и МСЭ-T X.683, с TTCN-3. В настоящей Рекомендации не рассматривается согласование других языков с TTCN-3.

Первый пересмотр Рекомендации содержит поправки (соответствие и совместимость; требования и описания, связанные с типом objid, были перенесены в данную Рекомендацию из всех других Рекомендаций МСЭ-Т серии МСЭ-Т Z.16x, поддержка значений XML в модулях ASN.1, преобразование типов OID-IRI и RELATIVE-OID-IRI, специальные действительные значения и подтипы, содержащие специальные значения и исключительные границы, обновленные предопределенные строки языка и т. д.), разъяснения (например, о видимости импортированных определений ASN.1, о правилах преобразования), исправления и редакционные правки.

В этом пересмотре Рекомендации содержатся поправки, разъяснения, исправления и редакционные правки.

− Z.168 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Преобразование CORBA IDL в TTCN-3*, где содержатся правила преобразования языка описания интерфейса (IDL) общей архитектуры брокера объектных запросов (CORBA) в язык TTCN-3 (как определено в Рекомендации МСЭ‑T Z.161), чтобы обеспечить возможность тестирования систем на основе CORBA. Принципы преобразования CORBA IDL в TTCN-3 могут также использоваться для преобразования языков спецификации интерфейсов других объектно-/компонентно-ориентированных технологий. Спецификация других преобразований выходит за рамки данной Рекомендации. В этом пересмотре Рекомендации содержатся поправки, разъяснения, исправления и редакционные правки.

− Z.169 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Использование схемы XML с TTCN-3*, где содержится определение правил отображения схемы W3C в TTCN-3, чтобы обеспечить возможность тестирования систем, интерфейсов и протоколов на основе XML. В этом пересмотре Рекомендации содержатся поправки, разъяснения, исправления и редакционные правки.

− Z.170 (пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Спецификация замечаний по документации TTCN-3*, где определена документация исходного кода TTCN-3 с использованием специальных комментариев по документации. В настоящем пересмотре Рекомендации Z.170 содержит поправки, разъяснения, исправления и редакционные правки.

− Z.171 (новая и пересмотренная), *Нотация для тестирования и управления тестированием версии 3: Использование JSON с TTCN-3*, где изложены правила определения схем для структур данных JSON в TTCN-3, чтобы обеспечить возможность тестирования систем, интерфейсов и протоколов на базе JSON, а также правила преобразования между TTCN-3 и JSON для обеспечения обмена данными TTCN-3 в формате JSON между различными системами.

– Z.Imp100 (пересмотренное), *Руководство пользователя Рекомендаций по языку спецификации и описания – Версия 3.0.2*, в котором содержится подборка сообщенных дефектов и проблем поддержания вместе с решениями по их устранению для Рекомендаций МСЭ-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 и Z.119, относящихся к языку спецификации и описания*.*

– Z.Imp100 (пересмотренное), *Руководство пользователя Рекомендаций по языку спецификации и описания – Версия 4.0.0*, в котором содержится подборка сообщенных дефектов и проблем поддержания вместе с решениями по их устранению для Рекомендаций МСЭ-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 и Z.119, относящихся к языку спецификации и описания*.*

### m) Вопрос 13/17 − Аспекты безопасности для интеллектуальной транспортной системы 2017−2020 гг.)/ Безопасность интеллектуальных транспортных систем (ИТС) (2021 г. −)

Группа Докладчика по Вопросу 13/17 была учреждена в сентябре 2017 года и занимается разработкой Рекомендаций по аспектам безопасности интеллектуальной транспортной системы (ИТС). Сюда относятся различные типы связи в транспортных средствах, между транспортными средствами, а также между транспортными средствами и фиксированными местоположениями.

В данном исследовательском периоде в рамках Вопроса 13/17 были разработаны шесть новых Рекомендаций:

– X.1371, *Угрозы безопасности для соединенных транспортных средств*, где описаны угрозы безопасности для соединенных транспортных средств и экосистемы транспортных средств.

– X.1372, *Руководящие указания по безопасности систем связи транспортного средства с различными объектами (V2X)*, где содержатся руководящие указанияпо безопасности связи транспортного средства с различными объектами (V2X). Определены возможные угрозы в среде связи V2X и установлены требования безопасности к связи V2X с учетом угроз. В данной Рекомендации также представлены примеры сценариев использования услуг безопасности связи V2X.

– X.1373, *Возможность безопасного обновления программного обеспечения для устройств связи в интеллектуальных транспортных системах*, где представлены процедуры безопасного обновления программного обеспечения между сервером обновления программного обеспечения и автомобилями с соответствующим управлением безопасностью. Настоящая Рекомендация может на практике использоваться в автомобильной промышленности и отраслях, связанных с ИТС, в качестве набора стандартных возможностей для передового опыта.

– X.1374, *Требования безопасности для внешних интерфейсов и устройств с возможностью доступа к транспортному средству*, где проведен анализ угроз безопасности соединенным транспортным средствам с двух сторон: угрозы интерфейсам, которые используются для взаимодействия между транспортным средством и его внешними устройствами, и угрозы внешним устройствам, которые взаимодействуют с транспортным средством. В Рекомендации МСЭ-Т X.1374 определены требования безопасности для таких внешних интерфейсов и внешних устройств с возможностью доступа к транспортному средству в среде сетей электросвязи для устранения выявленных угроз в зависимости от типа интерфейсов доступа. Интерфейсы и внешние устройства с возможностью доступа к транспортному средству включают систему удаленного доступа в транспортное средство без ключа (RKE) со смарт-ключом, диагностические инструменты и беспроводные электронные ключи, использующие порт бортовой диагностики II (OBD-II), телематические устройства управления с устройствами беспроводной связи и т. д.

– X.1375, *Руководящие указания в отношении системы обнаружения проникновений в бортовые автомобильные сети*, где установлены руководящие принципы в отношении системы обнаружения проникновений (IDS) для бортовых автомобильных сетей (IVN). В Рекомендации МСЭ-Т X.1375 основное внимание уделяется способам обнаружения проникновения и злонамеренных действий в IVN, таких как использующие сеть контроллера (CAN), которые не могут поддерживаться обычными IDS, развернутыми в настоящее время в интернете. В Рекомендации МСЭ-Т X.1375 включена классификация и анализ атак, нацеленных на IVN. Также предлагаются методики и руководящие указания по реализации для обнаружения вторжения и злонамеренных действий в IVN на основе CAN, которые не могут поддерживаться обычными.

– X.1376, *Механизм обнаружения относящегося к безопасности ненадлежащего поведения, использующий большие данные, для соединенных транспортных средств*, где описан механизм обнаружения относящегося к безопасности ненадлежащего поведения для соединенных транспортных средств в помощь заинтересованным сторонам при использовании автомобильных данных для повышения безопасности транспортных средств. С расширением возможности соединения транспортных средств возрастает количество уязвимостей вследствие развития сложных технологий. Такие уязвимости увеличивают число угроз для соединенных транспортных средств. Для оценки безопасности соединенных транспортных средств весьма полезен анализ большого количества автомобильных данных.

В данном исследовательском периоде Группа Докладчика по Вопросу 13/17 провела небольшой семинар-практикум по проблемам кибербезопасности при автоматическом вождении (Женева, 26 августа 2019 г.).

### n) Вопрос 14/17 − Аспекты безопасности технологии распределенного реестра (2018−2020 гг.)/Безопасность технологии распределенного реестра (DLT) (2021 г. −)

Группа Докладчика по Вопросу 14/17 была учреждена в марте 2018 года и занимается разработкой Рекомендаций по аспектам безопасности технологий распределенного реестра (DLT), известных как блокчейн. Сюда входит предоставление комплексных решений в области безопасности приложений и услуг на основе DLT.

В данном исследовательском периоде в рамках Вопроса 14/17 были разработаны девять новых Рекомендаций:

– X.1400, *Термины и определения, относящиеся к технологии распределенного реестра*, где содержится базовый набор терминов и определений, относящихся к технологии распределенного реестра (DLT). Определения дают основную характеристику термина и, где это целесообразно, включено примечание для дополнительных пояснений.

– X.1401, *Угрозы безопасности технологии распределенного реестра*, где определены возможные угрозы для различных функциональных компонентов системы распределенного реестра, таких как протокол, сеть и данные. Настоящую Рекомендацию можно считать эталонным базовым уровнем при проектировании или реализации системы DLT.

– X.1402, *Структура безопасности для технологии распределенного реестра*, где описаны возможности обеспечения безопасности, которые могут смягчить соответствующие угрозы безопасности, и представлена методика структуры безопасности, для того чтобы определить порядок использования этих возможностей обеспечения безопасности для смягчения угроз безопасности конкретной системы DLT.

– X.1403, *Руководящие указания по обеспечению безопасности при использовании технологии распределенного реестра для децентрализованного управления определением идентичности*. Технология распределенного реестра (DLT) и ее конкретные реализации, такие как блокчейн, предоставляют уникальную возможность использования инфраструктуры доверия и платформы, которая может быть полезна для создания доверенной федерации в целях обмена атрибутами и информацией об идентичности. В настоящей Рекомендации рассмотрены относящиеся к электросвязи вопросы конфиденциальности и безопасности при использовании данных DLT для управления определением идентичности.

– X.1404, *Гарантия безопасности технологии распределенного реестра*, определены три уровня гарантии безопасности для технологии распределенного реестра (DLT) с целью содействия проектированию и разработке механизмов обеспечения безопасности. Определены также десять компонентов гарантии безопасности, составляющие гарантию безопасности, и критерии и руководящие указания для достижения каждого из трех уровней для компонента гарантии безопасности. Наконец, представлено сопоставление конкретных угроз и компонентов гарантии безопасности.

– X.1405, *Угрозы безопасности и требования безопасности для услуг цифровых платежей на основе технологии распределенного реестра*. На основе анализа сценариев использования платежных услуг в Рекомендации X.1405 описана модель услуг, а также проведен анализ угроз и проблем безопасности, после чего определены требования безопасности для противодействия выявленным угрозам и вызовам.

– X.1406, *Угрозы безопасности для системы онлайнового голосования с использованием технологии распределенного реестра*, где определены угрозы безопасности для системы онлайнового голосования с использованием DLT на основе инфраструктуры электросвязи/ИКТ. Предложена эталонная модель системы онлайнового голосования с исопльзованием DLT на основе инфраструктуры электросвязи/ИКТ и проведен анализ угроз безопасности в процессе онлайнового голосования, описанного в моделях

– X.1407, *Требования безопасности для услуг цифрового доказательства целостности данных на основе технологии распределенного реестра*, где определены угрозы и требования безопасности для услуг цифрового доказательства целостности данных на основе технологии распределенного реестра (DLT).

– X.1408, *Угрозы безопасности и требования безопасности для доступа к данным и совместного использования данных на основе технологии распределенного реестра*, где определена эталонная модель для описания доступа к данным и совместного использования данных на основе технологии распределенного реестра (DLT). Определены объекты и их роли, а также угрозы безопасности для доступа к данным и совместного использования данных на основе DLT. Наряду с этим определены требования безопасности для противодействия выявленным угрозам безопасности.

### o) Вопрос 15/17 – Безопасность для/с помощью появляющихся технологий, включая квантовую безопасность

Вопрос 15/17 был учрежден в январе 2021 года и предназначен для разработки Рекомендаций по безопасности для/с помощью появляющихся технологий, включая квантовую безопасность. Вопрос 15/17 включает также механизм инкубации ИК17 (TP.inno), который обеспечивает управляемую гибкость при исследовании возникающих областей безопасности с целью защиты новых появляющихся услуг и приложений на базе электросвязи/ИКТ.

В данном исследовательском периоде в рамках Вопроса 15/17 были разработаны две новые Рекомендации и одно Исправление к Техническому отчету:

– X.1712, *Требования и меры безопасности для сетей квантового распределения ключей – Управление ключами,* где определены угрозы безопасности и требования безопасности для управления ключами в сетях квантового распределения ключей (QKDN), а также определены меры безопасности управления ключами, которые служат для выполнения требования безопасности.

– X.1770, *Технические руководящие указания по безопасным многопользовательским вычислениям*, где определены технические руководящие указания в отношении многопользовательских вычислений (MPC) и представлена техническая стандартная основа для заинтересованных сторон в области ИКТ, предназначенная для использования MPC с целью защиты данных в сценариях совместной работы с данными и анализа больших данных. Наряду с этим описаны приложения, для которых возможно использовать MPC, а также описано, каким образом МРС может служить эталоном для заинтересованных сторон в области ИКТ для разработки приложений MPC.

– Испр. 1 к TR.sec-qkd, *Соображения безопасности для сетей квантового распределения ключей,* где проводится замена соответствующих выражений, относящихся к "IT-защите", замена терминов "кубиты" на "квантовые состояния", "совместное волокно" на "совместное распространение", а также внесены изменения в соответствующий контент.

## 3.3 Отчет о деятельности ведущей исследовательской комиссии, ГИС, JCA, региональных групп и проектов

17-я Исследовательская комиссия является ведущей исследовательской комиссией по вопросам безопасности электросвязи, управления определением идентичности и языкам и методам описания. Работа ведущей исследовательской комиссии распределяется следующим образом:

– Безопасность – в ведении Вопроса 1/17;

– Управление определением идентичности – в рамках Вопроса 10/17;

– Языки и методы описания – в совместном ведении Вопроса 11/17 и Вопроса 12/17 до 2020 года и в ведении Вопроса 11/17 после 2021 года.

### 3.3.1 Деятельность ведущей исследовательской комиссии по вопросам безопасности

17-я Исследовательская комиссия была назначена ведущей исследовательской комиссией по вопросам безопасности в соответствии с Резолюцией 2 Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ-16).

В качестве ведущей исследовательской комиссии по вопросам безопасности электросвязи 17‑я Исследовательская комиссия отвечает за изучение соответствующих основных Вопросов в области безопасности. Кроме того, при консультации с другими соответствующими исследовательскими комиссиями и в необходимых случаях в сотрудничестве с другими органами по стандартам 17-я Исследовательская комиссия несет ответственность за определение и поддержание общей структуры и за координацию, поручение (с учетом мандатов исследовательских комиссий) и приоритезацию исследований, проводимых исследовательскими комиссиями, а также за обеспечение подготовки последовательных, полных и своевременных Рекомендаций.

В рамках ИК17 деятельность ведущей исследовательской комиссии по безопасности координируется Вопросом 1/17. Эта работа осуществляется в тесном сотрудничестве с другими исследовательскими комиссиями для определения и выработки решений по вопросам безопасности. Однако конкретные специальные знания и опыт для интеграции этих решений в отдельные разрабатываемые технологии могут быть предложены только в рамках Вопроса, в рамках которого ведутся разработки.

В качестве ведущей исследовательской комиссии по вопросам безопасности 17‑я Исследовательская комиссия осуществляет постоянное взаимодействие со всеми исследовательскими комиссиями МСЭ‑T, сталкивающимися с аспектом безопасности в своей работе. ИК17 также сотрудничает с широким кругом органов по стандартизации и форумов по ИКТ и безопасности электросвязи. Особое внимание уделяется предотвращению потенциальных конфликтов в работе, проводимой исследовательскими комиссиями и внешними органами.

Кроме того, в ходе каждого собрания 17-й Исследовательской комиссии проводятся совещания по координации вопросов безопасности, составлен список контактов по вопросам безопасности для всех исследовательских комиссий, деятельность которых связана с вопросами безопасности.

В том что касается вопросов, связанных с работой ИК17 как ведущей исследовательской комиссии, были получены и рассмотрены внутренние заявления о взаимодействии по вопросам безопасности от CITS МСЭ, КСТ МСЭ, ИК1 МСЭ-D, ИК2 МСЭ-D (Вопрос 3/2, Вопрос 5/2), КГРЭ МСЭ-D, ИК1 МСЭ‑R, ИК5 МСЭ-R, ИК6 МСЭ-R, РГ МСЭ-R (4C, 5A, 5B, 5C, 5D, 6C), FIGI МСЭ-T, ОГ МСЭ‑T (AI4EE, AI4H, AN, DFC, DLT, DPM, ML5G, NET2030, QIT4N, VM), JCA МСЭ‑Т (IMT2020, IoT и SC&C, MMeS, SDN), КСТ МСЭ-T, ИК МСЭ-T (2, 3, 5, 9, 11, 12, 13, 15, 16, 20) и КГСЭ МСЭ-T.

В том что касается вопросов, связанных с работой ИК17 как ведущей исследовательской комиссии, были рассмотрены внешние заявления о взаимодействии, полученные от 3GPP (SA3), BIPM, CEN-CENELEC JTC 19, ISG ЕТСИ (CIM, ETI, F5G, IPE, NIN, QSC, SAI), ETSI SAGE, TC ЕТСИ (CYBER, ITS, MTS), FIDO Alliance, IEEE 802.1, РГ по TLS IETF, ТК307 ИСО, ПК ОТК1 ИСО/МЭК (6, 27/РГ1-5, 29/РГ1), MEF, NIST, OASIS, OMA, oneM2M, SAE и W3C.

ИК17 направила внутренние заявления о взаимодействии в адрес CITS МСЭ, IPRAHG, ИК1 МСЭ-D, ИК2 МСЭ-D, КГРЭ МСЭ-D, ИК МСЭ-R (4, 5 (РГ 5A, 5D)), FIGI МСЭ-T, ОГ МСЭ‑T (AI4EE, DFC, DLT, NET2030, DPM, QIT4N, VM), JCA МСЭ‑Т (IMT2020, IoT и SC&C, MMeS, SDN), КСТ МСЭ-Т, ИК МСЭ-T (2, 3, 5, 9, 11, 12, 13, 15, 16, 20) и КГСЭ МСЭ-Т.

ИК17 направила внешние заявления о взаимодействии в адрес 3GPP (SA3), APT ASTAP, BSI, CEN‑CENELEC JTC 19, CIS, ISG ЕТСИ (CIM, MEC, QKD, ZSM; SAGE), TC ЕТСИ (CYBER, ITS, MTS)), Альянс FIDO, Ассоциация GSM (FASG, SIM), ИКАО, Инициатива Blockchain IEEE, IETF, IRTF, ТК ИСО (12, 20, 22, 37, 204, 307), РГ9 ОТК1 ИСО/МЭК, ПК ОТК1 ИСО/МЭК (6 (РГ10), 7, 27 (РГ1, РГ2, РГ3, РГ4, РГ5), 29, 38, 42), Инициативы Kantara, MEF, MITRE, NGMN, NIST, OASIS TC (CTI, OpenC2, Trust Elevation), OIX, oneM2M, ONF, OPIX Foundation, RAISE Forum, SAE, ЕЭК ООН, ВПС, W3C, ВОИС, ВОЗ.

В соответствии с Резолюцией 7 ВАСЭ-16 "*Сотрудничество с Международной организацией по стандартизации (ИСО) и Международной электротехнической комиссией (МЭК)*" 17‑я Исследовательская комиссия ведет онлайновую таблицу, которая отражает ее взаимосвязи с техническими комитетами (TК) ИСО и МЭК и подкомитетами (ПК) ОТК1 ИСО/МЭК, что также включает определение характера таких взаимосвязей, как совместная работа (например, общие или парные тексты), техническое сотрудничество на основе механизма взаимодействия или информационное взаимодействие.

ИК17 были организованы следующие семинары-практикумы:

– [второй совместный семинар-практикум МСЭ и ВОЗ по теме "Цифровые сертификаты COVID-19"](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/1126/Pages/default.aspx)  
виртуальный, 13 час. 00 мин. − 18 час. 00 мин. CEST, 26 ноября 2021 года;

– [совместный семинар-практикум МСЭ/ВОЗ по цифровому сертификату вакцинации](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/0811/Pages/default.aspx)   
виртуальный, 13 час. 00 мин. − 18 час. 00 мин. CEST, 11 августа 2021 года;

– "Децентрализованные идентификаторы и блокчейн" в рамках проводимой [БРЭ Недели появляющихся технологий](https://www.itu.int/en/ITU-D/Conferences/ET/2021/Pages/Programme.aspx) 2021 года  
виртуальный, 14 час. 00 мин. − 15 час. 00 мин., 8 июля 2021 года;

– [мини-семинар-практикум ИК17 по проблемам кибербезопасности при автоматическом вождении](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx)  
Женева, 14 час. 30 мин. – 17 час. 30 мин., 26 августа 2019 года;

– [семинар-практикум МСЭ по безопасности финансовых технологий](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190826/Pages/default.aspx)  
Женева, Швейцария, 26 августа 2019 года;

– [семинар-практикум МСЭ "Квантовые информационные технологии (QIT) для сетей"](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Pages/default.aspx)  
Шанхай, Китай, 5–7 июня 2019 года;

– [мини-семинар-практикум ИК17 по безопасности квантовой связи](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/Secure%20quantum%20communication.aspx)  
Женева, 14 час. 30 мин. – 17 час. 30 мин., 24 января 2019 года;

– [семинар-практикум МСЭ "Искусственный интеллект/машинное обучение и безопасность"](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190121/Pages/default.aspx)  
Женева, Швейцария, 21 января 2019 года;

– [семинар-практикум МСЭ по кибератакам повышенной сложности и программам-вымогателям](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx)   
Женева, Швейцария, 28 августа 2018 года;

– [семинар-практикум МСЭ по безопасности 5G](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx)  
Женева, Швейцария, 19 марта 2018 года;

– [семинар-практикум МСЭ "Аспекты безопасности интеллектуальных транспортных систем"](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Pages/default.aspx)  
Женева, Швейцария, 28 августа 2017 года;

– [семинар-практикум МСЭ по аспектам безопасности технологии блокчейн](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Pages/default.aspx)  
Женева, Швейцария, 21 марта 2017 года.

В частности, в плане работы ИК17 в области безопасности рассматриваются:

− выполнение Резолюций 7, 11, 18, 32, 40, 44, 50, 52, 54, 58, 64, 65, 67, 70, 73, 75, 76 77, 78, 84, 86, 89, 90, 92, 93, 94, 96, 97 и 98 ВАСЭ-16;

− выполнение Резолюций 101, 123, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200, и 201 ПК-18;

− выполнение Резолюций 23, 30, 34, 45, 47, 54, 63, 67, 69 и 80 ВКРЭ-17.

Был разработан план действий 17-й Исследовательской комиссии в поддержку Резолюций ПК-14/18, ВАСЭ-16, ВКРЭ-17, который обновляется на каждом ее собрании. На собрании в марте 2020 года ИК17 был назначен редактор для содействия ведению этой работы.

Кроме того, на веб-сайте 17-й Исследовательской комиссии ведется домашняя страница ведущей исследовательской комиссии по вопросам безопасности с прямыми ссылками на основные продукты и услуги в области безопасности.

ИК17 активно обновляет базу данных стандартов безопасности ИКТ, которая относится к утвержденным стандартам Дорожной карты по стандартам безопасности ИКТ, являющейся важным инструментом для разработчиков стандартов, позволяющим избегать дублирования.

Кроме того, ИК17 обновила Сборник материалов по безопасности, в котором представлена информация о проводимой в МСЭ-Т деятельности по стандартизации в сфере безопасности, включая каталог Рекомендаций МСЭ-Т, касающихся безопасности, и каталог утвержденных МСЭ-Т определений и сокращений, относящихся к безопасности.

Было опубликовано второе издание Технического отчета об эффективном использовании стандартов безопасности. Отчет предназначен для оказания помощи пользователям, особенно из развивающихся стран, в улучшении понимания значения использования связанных с безопасностью Рекомендаций МСЭ-Т в различных контекстах (например, бизнес, коммерция, правительство, отрасль).

Седьмое издание Руководства по безопасности было опубликовано как Технический отчет. Руководство по безопасности является одним из основных информационно-просветительских материалов МСЭ-Т, в котором в доступной форме освещается важная работа в области безопасности, выполняемая всеми исследовательскими комиссиями МСЭ-Т.

Исследовательские комиссии МСЭ-Т (помимо ИК17) достигли следующих результатов в своей работе по Рекомендациям в области безопасности:

Утвержденные рекомендации

| ИК | Рекомендация | Название |
| --- | --- | --- |
| ИК9 | J.1204 | Структура безопасности операционной системы "умного" телевидения |
| ИК13 | Y.2241 | Структура обслуживания для поддержки повсеместно распространенного самостоятельного обучения на базе веб-объектов |
| ИК13 | Y.2774 | Функциональные требования углубленной проверки пакетов в будущих сетях |
| ИК13 | Y.3051 | Базовые принципы надежной среды в инфраструктуре ИКТ |
| ИК13 | Y.3052 | Обзор обеспечения доверия для инфраструктур и услуг ИКТ |
| ИК13 | Y.3053 | Принципы организации надежных сетей с сетевыми доменами, ориентированными на доверие |
| ИК13 | Y.3054 | Основа для медийных услуг на основе доверия |
| ИК13 | Y.3055 | Структура основанного на доверии управления персональными данными |
| ИК13 | Y.3056 | Структура начальной загрузки устройств и приложений для открытого доступа к доверенным услугам в распределенных экосистемах |
| ИК13 | Y.3057 | Модель индекса доверия для инфраструктуры и услуг ИКТ |
| ИК13 | Y.3302 | Функциональная архитектура организации сетей с программируемыми параметрами |
| ИК13 | Y.3514 | Облачные вычисления – Структура и требования к доверенным межоблачным вычислениям |
| ИК13 | Y.3516 | Функциональная архитектура межоблачных вычислений |
| ИК13 | Y.3517 | Облачные вычисления – Обзор межоблачного управления доверием |
| ИК13 | Y.3650 | Структура определяемой большими данными организации сетей на базе углубленной проверки пакетов |
| ИК13 | Y.3802 | Сети квантового распределения ключей – Функциональная архитектура |
| ИК13 | Y.3803 | Сети квантового распределения ключей – Управление ключами |
| ИК13 | Y.3804 | Сети квантового распределения ключей – Контроль и управление |
| ИК13 | Y.3805 | Сети квантового распределения ключей – Управление организацией сетей с программируемыми параметрами |
| ИК13 | Y.3806 | Сети квантового распределения ключей –Требования к гарантии качества обслуживания |
| ИК15 | G.873.1 | Оптическая транспортная сеть (ОТС): Линейная защита |
| ИК15 | G.873.3 | Оптическая транспортная сеть (ОТС): Защита совместно используемой ячеистой сети |
| ИК15 | G.8132/Y.1383  (пересмотренная) | Кольцевая защита MPLS-TP |
| ИК15 | G.9978 | Унифицированные высокоскоростные приемопередатчики для организации проводных домашних сетей – Защищенный доступ |
| ИК16 | H.248.77 | Протокол управления шлюзом: Пакет и процедуры для протокола защищенной передачи данных в реальном времени (SRTP) |
| ИК20 | Y.4457 | Архитектурная структура для услуг в области транспортной безопасности |
| ИК20 | Y.4808 | Базовая архитектура цифрового объекта для борьбы с контрафакцией в IoT |
| ИК20 | Y.4810 | Требования к безопасности данных для гетерогенных устройств IoT |

Согласованные Добавления и Дополнения

| ИК | Номер | Название |
| --- | --- | --- |
| ИК13 | Добавление 44 к Рекомендациям серии Y.3100 | Стандартизация и деятельность по разработке программного обеспечения с открытыми исходными кодами, связанная с программизацией сетей IMT‑2020 |

Проекты Рекомендаций, по которым получено согласие

|  |  |  |
| --- | --- | --- |
| ИК | Номер | Название |
| ИК13 | Y.2086  (Y.DNI-fr) | Принципы и требования децентрализованной надежной сетевой инфраструктуры  *(получено согласие 16.07.2021 г.)* |
| ИК13 | Y.3807  (Y.QKDN-QoS-pa) | Сети квантового распределения ключей – приложения машинного обучения  *(получено согласие 10.12.2021 г.)* |
| ИК13 | Y.3808  (Y.QKDN-frint) | Структура интеграции сети квантового распределения ключей и сети безопасных хранилищ  *(получено согласие 10.12.2021 г.)* |
| ИК13 | Y.3809  (Y.QKDN-BM) | Сети квантового распределения ключей – Модели на базе бизнес-ролей  *(получено согласие 10.12.2021 г.)* |

### 3.3.2 Деятельность ведущей исследовательской комиссии по вопросам управления определением идентичности

17-я Исследовательская комиссия была назначена ведущей исследовательской комиссией по вопросам управления определением идентичности (IdM) в соответствии с Резолюцией 2 Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ-16).

В качестве ведущей исследовательской комиссией по вопросам управления определением идентичности 17-я Исследовательская комиссия отвечает за изучение соответствующих основных Вопросов по IdM. Кроме того, при консультации с другими соответствующими исследовательскими комиссиями и в необходимых случаях в сотрудничестве с другими органами по стандартам Исследовательская комиссия несет ответственность за определение и поддержание общей структуры и за координацию, поручение (с учетом мандатов исследовательских комиссий) и приоритезацию исследований, проводимых исследовательскими комиссиями, а также за обеспечение подготовки последовательных, полных и своевременных Рекомендаций.

В частности, 17-я Исследовательская комиссия отвечает за исследования, связанные с разработкой общей модели управления определением идентичности, которая не зависит от сетевых технологий и поддерживает безопасный обмен информацией об идентичности между объектами. Эта работа также включает в себя исследование процесса обнаружения авторитетных источников информации об идентичности; общие механизмы для соединения/функционального взаимодействия различных наборов форматов информации об идентичности; угроз управлению идентичностью, механизмов противодействия им, защиты информации, позволяющей установить личность (PII), и разработку механизмов обеспечения того, чтобы доступ к PII был разрешен только в случае необходимости.

Ниже приведена информация о состоянии работы в области IdM в исследовательских комиссиях МСЭ‑T:

Исследовательские комиссии МСЭ-Т (помимо ИК17) достигли следующих результатов, относящихся к их работе по Рекомендациям в области IdM:

Утвержденные Рекомендации

| ИК | Рекомендация | Название |
| --- | --- | --- |
| ИК3 ИК17 | D.1140 X.1261\*\*\* | Политическая основа, включая принципы для инфраструктуры цифровой идентичности |
| ИК2 | E.217rev | Морская связь – опознаватель судовой станции |
| ИК11 | Q.4063 | Структура тестирования систем идентификации, используемых в интернете вещей |
| ИК11 | Q.5052 | Решение проблемы мобильных устройств с дублированными уникальными идентификаторами |
| ИК15 | L.207 | Элементы пассивных узлов с автоматическим обнаружением идентификационной метки |
| ИК16 | H.273 | Не зависящие от метода кодирования кодовые точки для идентификации типа видеосигнала |
| ИК17 | X.1252rev | Базовые термины и определения в области управления определением идентичности |
| ИК17 | X.1403 | Руководящие указания по обеспечению безопасности при использовании технологии распределенного реестра для децентрализованного управления определением идентичности |
| ИК20 | Y.4805 | Требования к услуге идентификатора для обеспечения функциональной совместимости различных приложений "умного" города |
| ИК20 | Y.4476 | Структура преобразования на основе OID для транзакций распределенного реестра, назначенных ресурсам IoT |
| ИК20 | Y.4809 | Идентификаторы IoT для интеллектуальных транспортных систем |
| ИК20 | Y.4811 | Эталонная структура конвергированных услуг для идентификации и аутентификации устройств IoT в децентрализованной среде |
| \*\*\* Двойная нумерация D.1140 (ИК3) как X.1261 (ИК17) | | |

Кроме того, на веб-сайте 17-й Исследовательской комиссии ведется домашняя страница ведущей исследовательской комиссии по вопросам управления определением идентичности с прямыми ссылками на основные ресурсы.

### 3.3.3 Деятельность ведущей исследовательской комиссии по вопросам языков и методов описания

17-я Исследовательская комиссия была назначена ведущей исследовательской комиссией по вопросам языков и методов описания в соответствии с Резолюцией 2 Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ-16).

В качестве ведущей исследовательской комиссии по вопросам языков и методов описания 17‑я Исследовательская комиссия отвечает за следующие виды деятельности, касающейся языков и методов описания для электросвязи:

– предоставление членам МСЭ‑T и другим исследовательским комиссиям руководства по использованию языков и методов описания;

– ведение набора Рекомендаций и других руководящих указаний МСЭ‑T по языкам и методам описания, используемым для электросвязи;

– консультирование в отношении приемлемых языков, доступных по другим каналам, которые необходимо использовать, если соответствующий язык не определен Рекомендацией МСЭ‑T;

– взаимодействие с другими признанными органами, такими как IETF и OMG, которые используют или определяют дополнительные языки и методы описания.

Проводимая в рамках Вопросов 11/17 и 12/17 работа была результативной в области языков и методов описания для ASN.1, SDL, MSC, URN и TTCN. Прогрессу в работе способствовало широкое сотрудничество с другими исследовательскими комиссиями и организациями.

В рамках Вопроса 11/17 ведется совместная работа с РГ10 ПК6 ОТК1 ИСО/МЭК по абстрактной синтаксической нотации версии один (ASN.1), результаты которой публикуются в качестве общих текстов в Рекомендациях серий X.680/X.690/X.890. В [базу данных модулей ASN.1](http://www.itu.int/ITU-T/recommendations/fl.aspx?lang=1) продолжают поступать новые добавления, позволяющие разработчикам получать опубликованные спецификации ASN.1 с проверенным синтаксисом и в машиночитаемом виде. Эта база данных содержит около 900 модулей более 200 Рекомендаций МСЭ-Т и модули других ОРС, которые ими упоминаются.

Язык спецификации и описания (SDL-2010) используется для определения систем в качестве эталонных моделей в Рекомендациях и в качестве реализаций. Грамматика SDL-2010 определена в Z.101–Z.107, формальное определение содержится в Приложении F к Z.100. Группа Докладчика по Вопросу 12/17 обновила формальное определение. Задача этого исследования состояла в обнаружении и устранении неоднозначностей, ошибок и расхождений в текстах Z.101–Z.107. В отношении формального определения, полностью согласующегося с SDL-2010, 5 сентября 2019 года было получено согласие на утверждение в рамках АПУ. Тогда же было получено согласие на утверждение в рамках АПУ в отношении обновленных текстов Z.100–Z.107, в которых были устранены неоднозначности, ошибки и расхождения. Пересмотренное Z.Imp100 было согласовано 5 сентября 2019 года с пустым перечнем изменений, вносимых в тексты Z.100–Z.107, в отношении которых было получено согласие на утверждение в рамках АПУ, и с перечнем предыдущих версий текстов как действующих. Конечным результатом является более четко определенный SDL-2010, имеющий упорядоченное формальное определение. Никаких дальнейших работ в настоящее время не планируется.

Вопрос 12/17 тесно связан с деятельностью TC MTS ЕТСИ, и ведение Рекомендаций серий Z.160 и Z.170 по TTCN-3 осуществляется на совместной основе. Были утверждены три новых текста и 25 пересмотренных текстов.

Кроме того, на веб-сайте 17-й Исследовательской комиссии ведется домашняя страница ведущей исследовательской комиссии по вопросам языков и методов описания с обзором по каждому из языков.

### 3.3.4 Совместная координационная деятельность по управлению определением идентичности (JCA-IdM)

Деятельность Группы по совместной координационной деятельности по управлению определением идентичности (JCA-IdM), работавшей в предыдущий исследовательский период, была продолжена в данный исследовательский период по предложению и с одобрения КГСЭ. JCA-IdM провела четыре собрания во время собраний ИК17 в августе/сентябре 2017 года, марте 2018 года, августе/сентябре 2018 года, августе/сентябре 2019 года, апреле 2021 года и августе/сентябре 2021 года для координации работы МСЭ-Т по управлению идентичностью (IdM) с внутренними группами МСЭ-Т и с соответствующими внешними организациями, такими как Decentralized Identify Foundation, FIDO Alliance, РГ5 ПК27 ОТК1 ИСО/МЭК, ТК307 ИСО, Инициатива Kantara, Mobile Driving Licence, Рабочая группа NH-ISAC Identity, OASIS, OpenIdD Foundation, Sovrin Foundation, SSI Open Standards и ВПС.

### 3.3.5 Региональная группа 17-й Исследовательской комиссии для Африки (РегГр-АФР ИК17)

Региональная группа ИК17 для Африки (РегГр-АФР ИК17), созданная в апреле 2015 года в предшествующий исследовательский период, продолжала свою работу в этом исследовательском периоде. Она провела одно собрание в этом исследовательском периоде (2−3 апреля 2019 г.) в форме совместного собрания с РегГр-АРБ ИК17.

### 3.3.6 Региональная группа ИК17 МСЭ для Арабского региона (РегГр-АРБ ИК17)

На собрании ИК17 в марте 2017 года была создана Региональная группа ИК17 для Арабского региона (РегГр-АРБ ИК17). Ее первое собрание состоялось в Маскате, Оман, в декабре 2017 года, второе собрание состоялось в Кувейте в октябре 2018 года, третье – в Тунисе 2−3 апреля 2019 года. Третье собрание было проведено в форме совместного собрания с РегГр-АФР ИК17.

На всех собраниях региональных групп ИК17 Советником ИК17 давались рекомендации по устранению пробелов в стандартизации и проводились обучающие занятия ИК17. Участники из стран региона провели мозговой штурм по темам кибербезопасности и определили темы, представляющие особый интерес для дальнейшего изучения.

## 3.4 Проекты

Осуществляемые ИК17 проекты ASN.1 и OID продолжает оказывать помощь:

− существующим пользователям ASN.1 и идентификаторов объектов (OID) как в рамках, так и за рамками МСЭ-T (например, ИК16 МСЭ-T, ПК27 ОТК1 ИСО/МЭК, ТК215 ИСО, 3GPP, и т. д.);

− странам, в частности развивающимся странам, в создании национального регистрирующего органа для OID.

В рамках данных проектов обеспечивались выступления лекторов и предоставлялись учебные материалы, а также координировалось предоставление пользователям инструментальной поддержки и контента соответствующих веб-сайтов.

### 3.4.1 Проект ASN.1

В рамках проекта ASN.1, которым руководит Пол Торп, предоставляется поддержка пользователям ASN.1 (Рекомендации МСЭ-Т серий X.680, X.690 и X.890) как в МСЭ-Т, так и за его пределами (например, ИК16 МСЭ-Т, ПК27 ОТК1 ИСО/МЭК, ТК215 ИСО, ETSI LI, 3GPP и др.). Он также помогает БСЭ в ведении актуализированной базы данных модулей ASN.1, не имеющих ошибок. В базу данных модулей ASN.1 продолжают поступать новые добавления, позволяющие разработчикам получать опубликованные спецификации ASN.1 с проверенным синтаксисом и в машиночитаемом виде. Эта база данных содержит модули более 200 Рекомендаций МСЭ-Т и модули других ОРС, которые ими упоминаются.

В сотрудничестве с БСЭ ведется база данных, содержащая машиночитаемую копию существующей версии всех модулей ASN.1, включенных в Рекомендации МСЭ-Т. Создание онлайновой базы данных по модулям ASN.1 является инструментом для МСЭ-Т с высокой добавленной стоимостью по сравнению с другими организациями по стандартизации. Он позволяет повысить эффективность отрасли за счет экономии времени и средств. Выполнение соответствующих Рекомендаций МСЭ-Т требует применения электронного формата (использующего кодирование ASCII) для прямой обработки формальных определений в существующих инструментах. Получение кодирования ASCII на основе печатного или постскрипт-документа требует перепечатывания документа, препятствует быстрой реализации и может привести к ошибкам. Сосредоточение всех модулей ASN.1 в одном месте значительно облегчает внедрение соответствующих протоколов. База данных по ASN.1 содержит также некоторые модули нескольких других органов по стандартам.

### 3.4.2 Проект OID

OID являются средством универсального и однозначного указания на объекты, используемые или определенные в стандартах. В рамках Вопроса 11/17 продолжена работа по иерархической регистрации идентификаторов объекта (OID) МСЭ-Т (серии МСЭ-Т X.660 и X.670), которая будет активно разрабатываться совместно с ПК6 ОТК1 ИСО/МЭК.

Дерево международных OID насчитывает более 1 643 596 регистраций на 16 ноября 2021 года (<http://www.oid-info.com/cgi-bin/display?a=count_nodes>), записанных в репозитории OID по адресу <http://www.oid-info.com>, и обеспечивает идентификацию объектов (любого вида) через иерархическую схему распределения, которая контролируется совместно МСЭ-Т и ИСО/МЭК. OID дают возможность идентификации объектов с использованием любого языка в мире (структурированным и иерархическим образом).

В частности, была утверждена Рекомендация X.677 "*Механизм идентификации для беспилотных летательных аппаратов с использованием идентификаторов объектов*", содержащая результаты анализа требований к управлению полным жизненным циклом и распознаванию эксплуатационной идентичности беспилотных летательных аппаратов (БПЛА) с учетом соображений безопасности, и в ней был определен механизм идентификации БПЛА с использованием идентификаторов объектов (OID).

Проект OID, которым руководит г-н Оливье Дюбюиссон, оказывает помощь национальным администрациям, и национальные органы ИСО/МЭК создают орган регистрации для OID своих стран, в том числе Бахрейн, Бенин, Эквадор, Ямайка и Вьетнам.

## 3.5 Преодоление разрыва в стандартизации

На всех очных собраниях ИК17 в течение этого исследовательского периода БСЭ организовывало приветственный прием и экскурсию по помещениям МСЭ для новых участников ИК17. Председатель ИК17 провел ознакомительную сессию для новых участников ИК17 и беседу новых участников с руководством ИК17. В январе 2019 года Советник ИК17 организовал практикум Советника ИК17, на котором отвечал на вопросы делегатов ИК17 о методах работы ИК17. В сентябре 2019 года БСЭ организовало обучающее занятие для руководящего состава МСЭ-Т – Докладчиков и редакторов ИК17.

С марта 2017 года по сентябрь 2018 года ИК17 во время своих собраний регулярно проводила практические обучающие занятия для делегатов из развивающихся стран. На этих занятиях предоставлялось много информации о программе, видах деятельности и проектах МСЭ в области преодоления разрыва в стандартизации; они являются для развивающихся стран весьма подходящим местом, где они могут представить ИК17 свои предложения. Эти сессии служат для развивающихся стран катализатором для выражения своих интересов и потребностей.

В этом исследовательском периоде ИК17 регулярно организовывала неофициальные (электронные) встречи делегатов из Африки и арабских государств соответственно во время проведения (электронных) собраний ИК17 для содействия обсуждению планирования будущей работы РегГр-АФР ИК17 и РегГр-АРБ ИК17.

# 4 Замечания, касающиеся будущей работы

Деятельность 17-й Исследовательской комиссии в области безопасности продолжалась в течение данного исследовательского периода и заметно расширилась, и Комиссия является центром профессионального мастерства, специализирующимся в области безопасности. 17‑я Исследовательская комиссия − ведущая исследовательская комиссия Сектора стандартизации по вопросам безопасности. Создана база Рекомендаций/стандартов по безопасности, достигнуты договоренности о сотрудничестве и координации с другими органами, и в части II отчета 17-й Исследовательской комиссии предлагается программа текущей работы по Вопросам, связанным с безопасностью, на следующий исследовательский период. Учитывая, что укрепление доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ) является одним из важнейших приоритетов МСЭ, очень важно, чтобы такая компетенция МСЭ-Т в вопросах безопасности подкреплялась, расширялась и усиливалась, а не распылялась.

Необходимо противодействовать существующим и будущим угрозам и уязвимостям, затрагивающим безопасность, для укрепления доверия и безопасности при использовании ИКТ с учетом новых услуг и появляющихся приложений на основе сетей электросвязи/ИКТ, и для этого разрабатывать Рекомендации и Технические отчеты. Технологии безопасности являются важнейшими элементами защиты систем ИКТ от атак или повреждения оборудования, программного обеспечения или информации, а также от сбоев в предоставлении услуг и от использования предоставляемых ею услуг не по назначению.

Могут потребоваться новые подходы к безопасности и меры для адекватного реагирования на угрозы и риски безопасности. 17-й Исследовательской комиссии предстоит играть ключевую роль в разработке международных стандартов в области безопасности.

Безопасность и защита электросвязи и ИКТ остается областью, в которой будут требоваться стандарты безопасности. Управление новыми возникающими угрозами для электросвязи и ИКТ, включая сетевую инфраструктуру, системы, приложения и услуги, имеет критически важное значение. Понятна необходимость разработки реализуемых стандартов и руководящих указаний по безопасности, отвечающих потребностям всех стран.

Чрезвычайно важно обеспечивать управление новыми возникающими угрозами для инфраструктуры электросвязи и ИКТ. Проделанную 17-й Исследовательской комиссией работу в области безопасности (включая общую архитектуру безопасности, структуру, требования, механизмы, протоколы и руководящие указания по управлению для неоднородных сетей/систем/услуг) необходимо продолжить, и необходимо, чтобы была ведущая исследовательская комиссия по вопросам безопасности для координации деятельности в рамках МСЭ, а также с другими организациями по разработке стандартов (ОРС). 17-я Исследовательская комиссия осознает необходимость разработки реализуемых стандартов и руководящих указаний по безопасности, отвечающих потребностям всех стран.

Укрепление основ безопасности и защиты информации, позволяющей установить личность (PII), является необходимым условием развития информационного общества с высокой плотностью соединений и укрепления доверия, уверенности и безопасности среди пользователей информационно-коммуникационных технологий (ИКТ). Данные, используемые в приложениях и услугах, защищены соответствующими технологиями обеспечения безопасности, а также организационными и физическими мерами. Безопасность для и с помощью электросвязи и ИКТ остается областью, в которой будут необходимы стандарты безопасности. Новые появляющиеся технологии, такие как облачные вычисления (в том числе граничные облачные вычисления и многооблачные вычисления), "умные" электросети, интеллектуальные предприятия, интеллектуальные транспортные системы, сотовые сети пятого поколения и далее, сети с программируемыми параметрами, виртуализация сетевых функций, нарезка сетей, анализ больших данных, интернет вещей, технологии распределенного реестра, интеллектуальная транспортная система и квантовая безопасность требуют разработки технических и организационных мер по реагированию на различные угрозы и риски и защите PII граждан, а также технических и организационных мер по защите детей в онлайновой среде. Могут потребоваться новые подходы и меры, основанные на оценке рисков безопасности, для адекватного реагирования на угрозы и риски безопасности. 17‑й Исследовательской комиссии предстоит играть ключевую роль в разработке международных стандартов в этих областях. Необходимой разработкой подходов к безопасности для появляющихся технологий лучше всего заниматься в исследовательской комиссии, которая имеет специальные знания в сфере существующих подходов к безопасности.

Благодаря своей деятельности в качестве ведущей исследовательской комиссии в области безопасности и в результате деятельности ИК17 по взаимодействию и координации, ИК17 выполняет роль ведущего координатора и остается в курсе деятельности других исследовательских комиссий в области безопасности, а также работы других ОРС и консорциумов. Предполагается, что деятельность ИК17 в области взаимодействия и координации в будущем по-прежнему будет играть важную роль. ИК17 имеет успешный опыт сотрудничества с другими ОРС в совместной разработке Рекомендаций/стандартов. В целом ИК17 в своем качестве ведущей исследовательской комиссии и для того, чтобы лучше выполнять свою деятельность по стандартизации в области безопасности, эффективно использует средства взаимодействия (переписку, официальное сотрудничество на основе взаимодействия A.4/A.5/A.6), а также ссылки и совместную разработку (A.23/A.25).

Кроме того, ИК17 является ведущей исследовательской комиссией по управлению определением идентичности (IdM) − основным глобальным средством управления цифровыми идентичностями, установления доверия, защиты информации, позволяющей установить личность, эксплуатации сетей, включая управление доступом к сетям или услугам, осуществления электронных онлайновых транзакций, обеспечения работы финансовых технологий, ОТТ и оказания цифровых финансовых услуг и др. Поскольку управление определением идентичности играет столь важную роль в укреплении доверия и безопасности при использовании ИКТ, оно является неотъемлемой частью работы 17-й Исследовательской комиссии как ведущей исследовательской комиссии МСЭ-Т в области безопасности. ИК17 продолжает координировать работу в области IdM, включая децентрализованную идентичность на основе DLT, в МСЭ и с другими ОРС. Ее работа, связанная с PKI, ASN.1 и OID, полезна для многих секторов ИКТ.

Новые среды электросвязи/ИКТ, такие как интернет вещей (IoT), ИТС, интеллектуальные предприятия, "умные" города и сообщества, а также "умные" электросети, нуждаются в новых требованиях безопасности при использовании инфраструктуры открытых ключей (PKI). PKI первоначально была рассчитана только для защиты банковских операций и электронного правительства и не была предназначена для удовлетворения требований малоемких структур, миллионов и миллиардов структур, не требующих вмешательства человека. Если PKI не будет адаптирована к этим новым условиям, то важные аспекты безопасности IoT, интеллектуальных предприятий и "умных" электросетей окажутся неэффективными, что в значительной степени повлияет на общество и повседневную жизнь людей, поскольку отразится на стабильности большей части основных инфраструктур. Работа по совершенствованию PKI для удовлетворения требований новой среды должна пользоваться в следующем исследовательском периоде высоким приоритетом.

Для обеспечения эффективной безопасности потребуются новые стандарты. В МСЭ давно признается важность структурированных инструментов формулировок, таких как абстрактная синтаксическая нотация версии 1 (ASN.1). В случае ASN.1 значительный шаг вперед был сделан путем приведения ASN.1 в Рекомендациях МСЭ-Т в соответствие с определением ASN.1 и представления этого в виде файлов, пригодных для машинного считывания. Распространение такого подхода (и поддержание ресурсов МСЭ) на другие языки спецификации, такие как язык спецификации и описания (SDL), могло бы еще больше повысить безопасность, отличающую Рекомендации хорошего качества. Использование таких Рекомендаций было бы полезным для продуктов. Наряду с формальными языками для написания Рекомендаций, МСЭ предоставил также нотацию для тестирования и управления тестированием (TTCN) для описания проверок на соответствие (и других тестов).

# 5 Обновления к Резолюции 2 ВАСЭ на исследовательский период 2022−2024 годов

В Приложении 2 содержатся обновления к Резолюции 2 ВАСЭ, предложенные 17‑й Исследовательской комиссией в отношении заголовка, общих областей исследований, ведущих ролей, руководящих ориентиров и Рекомендаций на будущий исследовательский период.

ПРИЛОЖЕНИЕ 1

**Список Рекомендаций, Добавлений и других материалов, разработанных или исключенных в течение исследовательского периода**

Список новых и пересмотренных Рекомендаций, утвержденных в течение данного исследовательского периода, содержится в Таблице 7.

В Таблице 7 перечислены **Рекомендации**, **Поправки** и **Исправления**, утвержденные в течение данного исследовательского периода, по состоянию на 7 января 2022 года, дату составления этой таблицы. Тексты представлены в порядке расположения Рекомендаций (по алфавиту и порядковому номеру) и затем по датам утверждения (первыми следуют старые версии). Рекомендации с двойной нумерацией будут представлены один раз. Рекомендации, которыми занимаются другие исследовательские комиссии, будут представлены только в рамках той исследовательской комиссии, которая их утвердила.

В Таблице 8 приведен список Рекомендаций, по которым сделано заключение/получено согласие на последнем собрании 17‑й Исследовательской комиссии.

Тексты представлены в порядке расположения Рекомендаций (по алфавиту и порядковому номеру). Рекомендации с двойной нумерацией будут представлены один раз. Рекомендации, которыми занимаются другие исследовательские комиссии, будут представлены только в рамках той исследовательской комиссии, которая их утвердила.

ПРИМЕЧАНИЕ. – Под последним собранием в настоящем отчете понимается собрание, проходившее 7 января 2022 года.

В Таблице 9 приведен список Рекомендаций, которые были исключены 17-й Исследовательской комиссией в течение данного исследовательского ‎периода. Тексты представлены в порядке расположения Рекомендаций (по алфавиту и порядковому номеру). Рекомендации с двойной нумерацией будут представлены один раз.

В Таблице 10 приведен список Рекомендаций, представленных 17-й Исследовательской комиссией на утверждение ВАСЭ‑20.

В Таблице 11 и последующих таблицах приведены списки других публикаций, утвержденных и/или исключенных 17‑й Исследовательской комиссией в течение исследовательского ‎периода.

В Таблице 11 содержится перечень Добавлений, согласованных в течение данного исследовательского периода по состоянию на 7 января 2022 года, дату составления этой таблицы.

Таблица 7

17-я Исследовательская комиссия – Рекомендации, утвержденные в течение исследовательского периода

| Рекомендация | Утверждение | Статус | ТПУ/ АПУ | Название |
| --- | --- | --- | --- | --- |
| [X.500](http://handle.itu.int/11.1002/1000/14031) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Обзор понятий, моделей и услуг |
| [X.501](http://handle.itu.int/11.1002/1000/14032) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Модели |
| [X.501 (2019 г.) Попр. 1](http://handle.itu.int/11.1002/1000/14790) | 14.10.2021 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник − Модели – Поправка 1: Различные усовершенствования |
| [X.509](http://handle.itu.int/11.1002/1000/14033) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов |
| [X.509 (2019 г.)  Испр. 1](http://handle.itu.int/11.1002/1000/14791) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник – Структуры сертификатов открытых ключей и атрибутов: Исправление 1 |
| [X.510](http://handle.itu.int/11.1002/1000/14320) | 22.08.2020 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Спецификация протокола для безопасных операций |
| [X.511](http://handle.itu.int/11.1002/1000/14034) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Определение абстрактной службы |
| [X.518](http://handle.itu.int/11.1002/1000/14035) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Процедуры распределенных операций |
| [X.519](http://handle.itu.int/11.1002/1000/14036) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Спецификации протоколов |
| [X.520](http://handle.itu.int/11.1002/1000/14037) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Избранные типы атрибутов |
| [X.521](http://handle.itu.int/11.1002/1000/14038) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Избранные объектные классы |
| [X.525](http://handle.itu.int/11.1002/1000/14047) | 14.10.2019 г. | Действующая | АПУ | Информационные технологии – Взаимосвязь открытых систем – Справочник: Копирование |
| [X.676](http://handle.itu.int/11.1002/1000/13712) | 29.11.2018 г. | Действующая | АПУ | Структура разрешения на базе идентификатора объекта для сгруппированных услуг IoT |
| [X.677](http://handle.itu.int/11.1002/1000/14039) | 08.03.2020 г. | Действующая | АПУ | Механизм идентификации для беспилотных летательных аппаратов с использованием идентификаторов объектов |
| [X.680 (2015 г.) Испр.1](http://handle.itu.int/11.1002/1000/13257) | 14.05.2017 г. | Замененная | АПУ |  |
| [X.680 (2015 г.) Испр.2](http://handle.itu.int/11.1002/1000/13361) | 14.10.2017 г. | Замененная | АПУ |  |
| [X.680 (2015 г.) Испр.3](http://handle.itu.int/11.1002/1000/13598) | 14.05.2018 г. | Замененная | АПУ |  |
| [X.680 (2015 г.) Попр.1](http://handle.itu.int/11.1002/1000/13597) | 14.05.2018 г. | Замененная | АПУ | Смягчение пункта IMPORTS, для того чтобы разрешить импорт определений из новых версий конкретного модуля |
| [X.680](http://handle.itu.int/11.1002/1000/14468) | 13.02.2021 г. | Действующая | АПУ | Информационная технология – Абстрактная синтаксическая нотация № 1 (ASN.1): Спецификация базовой нотации |
| [X.681 (2015 г.) Испр.1](http://handle.itu.int/11.1002/1000/13599) | 14.05.2018 г. | Замененная | АПУ |  |
| [X.681](http://handle.itu.int/11.1002/1000/14469) | 13.02.2021 г. | Действующая | АПУ | Информационная технология – Абстрактная синтаксическая нотация № 1 (ASN.1): Спецификация информационных объектов |
| [X.682 (2015 г.) Испр.1](http://handle.itu.int/11.1002/1000/13362) | 14.10.2017 г. | Замененная | АПУ |  |
| [X.682 (2015 г.) Испр.2](http://handle.itu.int/11.1002/1000/13600) | 14.05.2018 г. | Замененная | АПУ |  |
| [X.682](http://handle.itu.int/11.1002/1000/14470) | 13.02.2021 г. | Действующая | АПУ | Информационная технология – Абстрактная синтаксическая нотация № 1 (ASN.1): Спецификация ограничений |
| [X.683 (2015 г.) Испр.1](http://handle.itu.int/11.1002/1000/13601) | 14.05.2018 г. | Замененная | АПУ |  |
| [X.683](http://handle.itu.int/11.1002/1000/14471) | 13.02.2021 г. | Действующая | АПУ | Информационная технология – Абстрактная синтаксическая нотация № 1 (ASN.1): Параметризация спецификаций ASN.1 |
| [X.690](http://handle.itu.int/11.1002/1000/14472) | 13.02.2021 г. | Действующая | АПУ | Информационная технология – Правила кодирования ASN.1: Спецификация базовых правил кодирования (BER), канонических правил кодирования (CER) и отличительных правил кодирования (DER) |
| [X.691](http://handle.itu.int/11.1002/1000/14473) | 13.02.2021 г. | Действующая | АПУ | Информационная технология – Правила кодирования ASN.1: Спецификация правил пакетного кодирования (PER) |
| [X.692](http://handle.itu.int/11.1002/1000/14474) | 13.02.2021 г. | Действующая | АПУ | Информационная технология – Правила кодирования ASN.1: Спецификация нотации управления кодированием (ECN) |
| [X.693 (2015 г.) Испр.1](http://handle.itu.int/11.1002/1000/13363) | 14.10.2017 г. | Замененная | АПУ |  |
| [X.693](http://handle.itu.int/11.1002/1000/14475) | 13.02.2021 г. | Действующая | АПУ | Информационная технология – Правила кодирования ASN.1: Правила кодирования языка XML (XER) |
| [X.694 (2015 г.) Испр.1](http://handle.itu.int/11.1002/1000/14040) | 14.10.2019 г. | Замененная | АПУ |  |
| [X.694](http://handle.itu.int/11.1002/1000/14476) | 13.02.2021 г. | Действующая | АПУ | Информационные технологии – Правила кодирования ASN.1: Отображение определений схемы языка XML консорциума W3C в системе обозначений ASN.1 |
| [X.695](http://handle.itu.int/11.1002/1000/14477) | 13.02.2021 г. | Действующая | АПУ | Информационная технология – Правила кодирования ASN.1: Регистрация и применение инструкций по кодированию PER |
| [X.696 (2015 г.) Испр.1](http://handle.itu.int/11.1002/1000/13258) | 14.05.2017 г. | Замененная | АПУ |  |
| [X.696 (2015 г.) Испр.2](http://handle.itu.int/11.1002/1000/13364) | 14.10.2017 г. | Замененная | АПУ |  |
| [X.696 (2015 г.) Испр.3](http://handle.itu.int/11.1002/1000/13602) | 14.05.2018 г. | Замененная | АПУ |  |
| [X.696](http://handle.itu.int/11.1002/1000/14478) | 13.02.2021 г. | Действующая | АПУ | Информационные технологии – Правила кодирования ASN.1: Спецификация правил кодирования по октетам (OER) |
| [X.697](http://handle.itu.int/11.1002/1000/13365) | 14.10.2017 г. | Замененная | АПУ | Информационные технологии – Правила кодирования ASN.1: Спецификация правил кодирования нотации объектов JavaScript (JER) |
| [X.697](http://handle.itu.int/11.1002/1000/13365) | 13.02.2021 г. | Действующая | АПУ | Информационные технологии – Правила кодирования ASN.1: Спецификация правил кодирования нотации объектов JavaScript (JER) |
| [X.893 (2007 г.) Испр.1](http://handle.itu.int/11.1002/1000/14041) | 14.10.2019 г. | Действующая | АПУ |  |
| [X.894](http://handle.itu.int/11.1002/1000/12848) | 14.10.2018 г. | Действующая | АПУ | Информационные технологии – Общие приложения ASN.1 – Синтаксис криптографических сообщений |
| [X.894 (2018 г.) Испр.1](http://handle.itu.int/11.1002/1000/13871) | 16.03.2019 г. | Действующая | АПУ |  |
| [X.894 (2018 г.) Испр. 2](http://handle.itu.int/11.1002/1000/14467) | 13.02.2021 г. | Действующая | АПУ | Общие приложения ASN.1 – Синтаксис криптографических сообщений – Техническое исправление 2 |
| [X.1011](http://handle.itu.int/11.1002/1000/14793) | 29.10.2021 г. | Действующая | АПУ | Руководящие указания по обеспечению непрерывной защиты процесса доступа к услуге |
| [X.1040](http://handle.itu.int/11.1002/1000/13366) | 14.10.2017 г. | Действующая | АПУ | Эталонная архитектура безопасности для управления жизненным циклом бизнес-данных электронной коммерции |
| [X.1041](http://handle.itu.int/11.1002/1000/13603) | 14.05.2018 г. | Действующая | АПУ | Структура безопасности работы сети для передачи голоса на основе технологии долгосрочного развития (VoLTE) |
| [X.1042](http://handle.itu.int/11.1002/1000/13803) | 30.01.2019 г. | Действующая | ТПУ | Службы безопасности, использующие сети с программируемыми параметрами |
| [X.1043](http://handle.itu.int/11.1002/1000/13872) | 16.03.2019 г. | Действующая | АПУ | Структура и требования безопасности для создания цепочек функций услуг на базе сетей с программируемыми параметрами |
| [X.1044](http://handle.itu.int/11.1002/1000/14042) | 29.10.2019 г. | Действующая | АПУ | Требования безопасности виртуализации сетей |
| [X.1045](http://handle.itu.int/11.1002/1000/14043) | 29.10.2019 г. | Действующая | АПУ | Архитектура цепочки услуг безопасности для сетей и приложений |
| [X.1046](http://handle.itu.int/11.1002/1000/14442) | 14.12.2020 г. | Действующая | АПУ | Структура безопасности с программируемыми параметрами в сетях с программируемыми параметрами/сетях с виртуализацией сетевых функций |
| [X.1047](http://handle.itu.int/11.1002/1000/14794) | 29.10.2021 г. | Действующая | АПУ | Требования и архитектура безопасности для управления отрезками сети и их оркестровки |
| [X.1051 (2016 г.) Испр.1](http://handle.itu.int/11.1002/1000/13407) | 06.09.2017 г. | Действующая | Согла-сование |  |
| [X.1052](http://handle.itu.int/11.1002/1000/14044) | 29.10.2020 г. | Действующая | АПУ | Процессы управления информационной безопасностью для организаций электросвязи |
| [X.1053](http://handle.itu.int/11.1002/1000/13367) | 13.11.2017 г. | Действующая | АПУ | Свод правил по управлению информационной безопасностью на основе МСЭ-T X.1051 для малых и средних организаций электросвязи |
| [X.1058](http://handle.itu.int/11.1002/1000/13182) | 30.03.2017 г. | Действующая | ТПУ | Информационные технологии – Методы обеспечения безопасности – Свод правил и норм для защиты информации, позволяющей установить личность |
| [X.1059](http://handle.itu.int/11.1002/1000/14045) | 29.10.2019 г. | Действующая | АПУ | Руководство по внедрению в организациях электросвязи управления рисками в отношении своих активов, доступных по глобальным сетям на базе IP |
| [X.1060](http://handle.itu.int/11.1002/1000/14721) | 29.06.2021 г. | Действующая | АПУ | Структура для создания и эксплуатации центра по защите от киберугроз |
| [X.1061](http://handle.itu.int/11.1002/1000/14733) | 22.08.2021 г. | Действующая | АПУ | Руководство по приобретению киберстрахования |
| [X.1080.0](http://handle.itu.int/11.1002/1000/13193) | 30.03.2017 г. | Действующая | ТПУ | Управление доступом для защиты телебиометрических данных |
| [X.1080.0 (2017 г.) Испр.1](http://handle.itu.int/11.1002/1000/13591) | 29.03.2018 г. | Действующая | Согла-сование |  |
| [X.1080.1](http://handle.itu.int/11.1002/1000/13604) | 14.05.2018 г. | Действующая | АПУ | Электронное здравоохранение и всемирная телемедицина – Общий протокол электросвязи |
| [X.1080.2](http://handle.itu.int/11.1002/1000/14795) | 29.10.2021 г. | Действующая | АПУ | Протокол биология-машина (B2M) |
| [X.1093](http://handle.itu.int/11.1002/1000/13725) | 13.11.2018 г. | Действующая | АПУ | Телебиометрический контроль доступа с "умными" идентификационными картами |
| [X.1094](http://handle.itu.int/11.1002/1000/13873) | 16.03.2019 г. | Действующая | АПУ | Телебиометрическая аутентификация с использованием биосигналов |
| [X.1126](http://handle.itu.int/11.1002/1000/13194) | 30.03.2017 г. | Действующая | ТПУ | Руководящие указания по смягчению негативных последствий от зараженных терминалов в сетях подвижной связи |
| [X.1127](http://handle.itu.int/11.1002/1000/13259) | 06.09.2017 г. | Действующая | ТПУ | Функциональные требования безопасности и функциональная архитектура для мер противодействия кражам мобильных телефонов |
| [X.1145](http://handle.itu.int/11.1002/1000/13260) | 14.05.2017 г. | Действующая | АПУ | Структура и требования безопасности для открытых возможностей услуг электросвязи |
| [X.1146](http://handle.itu.int/11.1002/1000/13368) | 14.10.2017 г. | Действующая | АПУ | Руководящие принципы обеспечения защиты для дополнительных услуг, предоставляемых операторами электросвязи |
| [X.1147](http://handle.itu.int/11.1002/1000/13726) | 13.11.2018 г. | Действующая | АПУ | Требования и структура безопасности для аналитики больших данных в услугах мобильного интернета |
| [X.1148](http://handle.itu.int/11.1002/1000/14249) | 03.09.2020 г. | Действующая | ТПУ | Структура процесса деидентификации для поставщиков услуг электросвязи |
| [X.1149](http://handle.itu.int/11.1002/1000/14250) | 29.05.2020 г. | Действующая | АПУ | Структура безопасности открытой платформы для услуг в сфере финансовых технологий |
| [X.1197 (2012 г.) Попр. 1](http://handle.itu.int/11.1002/1000/14046) | 05.09.2019 г. | Действующая | Согла-сование |  |
| [X.1212](http://handle.itu.int/11.1002/1000/13195) | 30.03.2017 г. | Действующая | ТПУ | Проектные решения для улучшенного восприятия конечным пользователем показателей благонадежности |
| [X.1213](http://handle.itu.int/11.1002/1000/13261) | 06.09.2017 г. | Действующая | ТПУ | Требования к возможностям обеспечения безопасности для противодействия  бот-сетям, использующим смартфоны |
| [X.1214](http://handle.itu.int/11.1002/1000/13404) | 29.03.2018 г. | Действующая | ТПУ | Методы оценки безопасности в сетях электросвязи/информационно-коммуникационных технологий |
| [X.1215](http://handle.itu.int/11.1002/1000/13849) | 30.01.2019 г. | Действующая | ТПУ | Сценарии использования структурированного представления информации об угрозах |
| [X.1216](http://handle.itu.int/11.1002/1000/14259) | 03.09.2020 г. | Действующая | ТПУ | Требования к сбору и сохранению доказательств по инцидентам кибербезопасности |
| [X.1217](http://handle.itu.int/11.1002/1000/14443) | 07.01.2021 г. | Действующая | ТПУ | Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи |
| [X.1218](http://handle.itu.int/11.1002/1000/14444) | 29.10.2020 г. | Действующая | АПУ | Требования и руководящие указания по динамическому анализу вредоносного программного обеспечения в изолированной среде |
| [X.1232](http://handle.itu.int/11.1002/1000/14085) | 29.10.2019 г. | Действующая | АПУ | Техническая основа противодействия рекламному спаму в информации, генерируемой пользователями |
| [X.1233](http://handle.itu.int/11.1002/1000/14773) | 03.09.2021 г. | Действующая | ТПУ | Руководящие указания по противодействию распространению спама при мгновенном обмене сообщениями |
| [X.1234](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14796&lang=en) | 07.01.2022 г. | Действующая | ТПУ | Руководящие указания по противодействию распространению спама с использованием услуг передачи мультимедийных сообщений (MMS) |
| [X.1235](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14797&lang=en) | 07.01.2022 г. | Действующая | ТПУ | Технологии противодействия подделке веб-сайтов, предназначенные для организаций электросвязи |
| [X.1248](http://handle.itu.int/11.1002/1000/13262) | 06.09.2017 г. | Действующая | ТПУ | Технические требования для противодействия распространению спама  при мгновенном обмене сообщениями |
| [X.1249](http://handle.itu.int/11.1002/1000/13605) | 30.01.2019 г. | Действующая | ТПУ | Техническая основа противодействия рекламному спаму в приложениях для мобильных устройств |
| [X.1252](http://handle.itu.int/11.1002/1000/14642) | 30.04.2021 г. | Действующая | ТПУ | Базовые термины и определения в области управления определением идентичности |
| [X.1254](http://handle.itu.int/11.1002/1000/14260) | 03.09.2020 г. | Действующая | ТПУ | Структура гарантии аутентификации объекта |
| [X.1276](http://handle.itu.int/11.1002/1000/13606) | 14.05.2018 г. | Действующая | АПУ | Протокол и метаданные поэтапной аутентификации, версия 1.0 |
| [X.1277](http://handle.itu.int/11.1002/1000/13727) | 29.11.2018 г. | Действующая | АПУ | Структура универсальной аутентификации |
| [X.1278](http://handle.itu.int/11.1002/1000/13728) | 29.11.2018 г. | Действующая | АПУ | Протокол клиент-аутентификатор/ универсальная двухфакторная схема |
| [X.1279](http://handle.itu.int/11.1002/1000/14261) | 03.09.2020 г. | Действующая | ТПУ | Система расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения |
| [X.1331](http://handle.itu.int/11.1002/1000/13405) | 29.03.2018 г. | Действующая | ТПУ | Руководящие указания по безопасности для устройств домашней сети (HAN) в системах "умных" электросетей |
| [X.1332](http://handle.itu.int/11.1002/1000/14086) | 26.03.2020 г. | Действующая | ТПУ | Руководящие указания по безопасности услуг интеллектуального учета в "умных" электросетях |
| [X.1333](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14798&lang=en) | 07.01.2022 г. | Действующая | ТПУ | Руководящие указания по безопасности для использования инструментов удаленного доступа в системах управления, подключенных к интернету |
| [X.1361](http://handle.itu.int/11.1002/1000/13607) | 07.09.2018 г. | Действующая | ТПУ | Структура безопасности интернета вещей на основе модели с использованием шлюза |
| [X.1362](http://handle.itu.int/11.1002/1000/13196) | 30.03.2017 г. | Действующая | ТПУ | Простая процедура шифрования для среды интернета вещей (IoT) |
| [X.1363](http://handle.itu.int/11.1002/1000/14087) | 29.05.2020 г. | Действующая | ТПУ | Техническая структура обработки информации, позволяющей установить личность, в среде интернета вещей |
| [X.1364](http://handle.itu.int/11.1002/1000/14088) | 26.03.2020 г. | Действующая | ТПУ | Требования безопасности и структура безопасности узкополосного интернета вещей |
| [X.1365](http://handle.itu.int/11.1002/1000/14089) | 26.03.2020 г. | Действующая | ТПУ | Методика обеспечения безопасности при использовании криптографии на основе идентичности в поддержку услуг интернета вещей (IoT) в сетях электросвязи |
| [X.1366](http://handle.itu.int/11.1002/1000/14262) | 03.09.2020 г. | Действующая | ТПУ | Схемы совокупной аутентификации сообщений для среды интернета вещей |
| [X.1367](http://handle.itu.int/11.1002/1000/14263) | 03.09.2020 г. | Действующая | ТПУ | Стандартный формат журналов регистрации ошибок в интернете вещей (IoT) для операций, связанных с инцидентами безопасности |
| [X.1368](http://handle.itu.int/11.1002/1000/14445) | 07.01.2021 г. | Действующая | ТПУ | Безопасное обновление микропрограммного или программного обеспечения устройств интернета вещей |
| [X.1369](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14799&lang=en) | 07.01.2022 г. | Действующая | ТПУ | Требования безопасности для платформы услуг IoT |
| [X.1371](http://handle.itu.int/11.1002/1000/14090) | 29.05.2020 г. | Действующая | ТПУ | Угрозы безопасности для соединенных транспортных средств |
| [X.1372](http://handle.itu.int/11.1002/1000/14091) | 26.03.2020 г. | Действующая | ТПУ | Руководящие указания по безопасности систем связи транспортного средства с различными объектами (V2X) |
| [X.1373](http://handle.itu.int/11.1002/1000/13197) | 30.03.2017 г. | Действующая | ТПУ | Возможность безопасного обновления программного обеспечения для устройств связи в интеллектуальных транспортных системах |
| [X.1374](http://handle.itu.int/11.1002/1000/14446) | 29.10.2020 г. | Действующая | АПУ | Требования безопасности для внешних интерфейсов и устройств с возможностью доступа к транспортному средству |
| [X.1375](http://handle.itu.int/11.1002/1000/14447) | 29.10.2020 г. | Действующая | АПУ | Руководящие указания в отношении системы обнаружения проникновений в бортовые автомобильные сети |
| [X.1376](http://handle.itu.int/11.1002/1000/14448) | 07.01.2021 г. | Действующая | ТПУ | Механизм обнаружения относящегося к безопасности ненадлежащего поведения, использующий большие данные, для соединенных транспортных средств |
| [X.1400](http://handle.itu.int/11.1002/1000/14449) | 29.10.2020 г. | Действующая | АПУ | Термины и определения, относящиеся к технологии распределенного реестра |
| [X.1401](http://handle.itu.int/11.1002/1000/14092) | 29.11.2019 г. | Действующая | АПУ | Угрозы безопасности технологии распределенного реестра |
| [X.1402](http://handle.itu.int/11.1002/1000/14251) | 22.07.2022 г. | Действующая | АПУ | Структура безопасности для технологии распределенного реестра |
| [X.1403](http://handle.itu.int/11.1002/1000/14264) | 03.09.2020 г. | Действующая | ТПУ | Руководящие указания по обеспечению безопасности при использовании технологии распределенного реестра для децентрализованного управления определением идентичности |
| [X.1404](http://handle.itu.int/11.1002/1000/14450) | 29.10.2020 г. | Действующая | АПУ | Гарантия безопасности технологии распределенного реестра |
| [X.1405](http://handle.itu.int/11.1002/1000/14722) | 29.06.2021 г. | Действующая | АПУ | Угрозы безопасности и требования безопасности для услуг цифровых платежей на основе технологии распределенного реестра |
| [X.1406](http://handle.itu.int/11.1002/1000/14734) | 14.07.2021 г. | Действующая | АПУ | Угрозы безопасности для системы онлайнового голосования с использованием технологии распределенного реестра |
| [X.1407](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14800&lang=en) | 07.01.2022 г. | Действующая | ТПУ | Требования безопасности для услуг цифрового доказательства целостности данных на основе технологии распределенного реестра |
| [X.1408](http://handle.itu.int/11.1002/1000/14801) | 29.10.2021 г. | Действующая | АПУ | Угрозы безопасности и требования безопасности для доступа к данным и совместного использования данных на основе технологии распределенного реестра |
| [X.1450](http://handle.itu.int/11.1002/1000/13729) | 14.10.2018 г. | Действующая | АПУ | Руководящие принципы для гибридной аутентификации и механизмов управления ключами в модели клиент-сервер |
| [X.1451](http://handle.itu.int/11.1002/1000/14252) | 29.05.2020 г. | Действующая | АПУ | Выявление рисков с целью оптимизации аутентификации |
| [X.1452](http://handle.itu.int/11.1002/1000/14451) | 29.10.2020 г. | Действующая | АПУ | Руководящие указания в отношении услуг безопасности, предоставляемых операторами |
| [X.1453](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14802&lang=en) | 07.01.2022 г. | Действующая | ТПУ | Угрозы безопасности и требования безопасности для систем управления видео |
| [X.1470](http://handle.itu.int/11.1002/1000/14803) | 13.11.2021 г. | Действующая | АПУ | Руководящие указания по безопасности веб-ориентированной онлайновой службы поддержки клиентов |
| [X.1500 (2011 г.) Попр. 11](http://handle.itu.int/11.1002/1000/13263) | 30.03.2017 г. | Замененная | Согла-сование | Пересмотренные методы обмена структурированной информацией о кибербезопасности |
| [X.1500 (2011 г.) Попр. 12](http://handle.itu.int/11.1002/1000/13590) | 29.03.2018 г. | Действующая | Согла-сование | Пересмотренные методы обмена структурированной информацией о кибербезопасности |
| [X.1541](http://handle.itu.int/11.1002/1000/13264) | 06.09.2017 г. | Действующая | ТПУ | Формат обмена описаниями инцидентов как объектов, версия 2 |
| [X.1550](http://handle.itu.int/11.1002/1000/13198) | 30.03.2017 г. | Действующая | ТПУ | Модели контроля доступа для сетей обмена информацией об инцидентах |
| [X.1603](http://handle.itu.int/11.1002/1000/13406) | 29.03.2018 г. | Действующая | ТПУ | Требования к безопасности данных для услуги мониторинга облачных вычислений |
| [X.1604](http://handle.itu.int/11.1002/1000/14093) | 26.03.2020 г. | Действующая | ТПУ | Требования безопасности к сети как услуге (NaaS) в среде облачных вычислений |
| [X.1605](http://handle.itu.int/11.1002/1000/14094) | 26.03.2020 г. | Действующая | ТПУ | Требования безопасности к открытой инфраструктуре как услуге (IaaS) в среде облачных вычислений |
| [X.1606](http://handle.itu.int/11.1002/1000/14265) | 03.09.2020 г. | Действующая | ТПУ | Требования к безопасности прикладной среды связи как услуги |
| [X.1643](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14804&lang=en) | 07.01.2022 г. | Действующая | ТПУ | Требования безопасности и руководящие указания по безопасности контейнеров виртуализации в среде облачных вычислений |
| [X.1702](http://handle.itu.int/11.1002/1000/14095) | 13.11.2019 г. | Действующая | АПУ | Архитектура генератора случайных чисел квантового шума |
| [X.1710](http://handle.itu.int/11.1002/1000/14452) | 29.10.2020 г. | Действующая | АПУ | Структура безопасности сетей квантового распределения ключей |
| [X.1712](http://handle.itu.int/11.1002/1000/14805) | 29.10.2021 г. | Действующая | АПУ | Требования и меры безопасности для сетей квантового распределения ключей |
| [X.1714](http://handle.itu.int/11.1002/1000/14453) | 29.10.2020 г. | Действующая | АПУ | Комбинация ключей и секретная доставка ключей для сетей квантового распределения ключей |
| [X.1750](http://handle.itu.int/11.1002/1000/14266) | 03.09.2020 г. | Действующая | ТПУ | Руководящие указания по безопасности больших данных как услуги для поставщиков услуг больших данных |
| [X.1751](http://handle.itu.int/11.1002/1000/14267) | 03.09.2020 г. | Действующая | ТПУ | Руководящие указания по обеспечению безопасности при управлении жизненным циклом больших данных для операторов электросвязи |
| [X.1752](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14806&lang=en) | 07.01.2022 г. | Действующая | ТПУ | Руководящие указания по безопасности для инфраструктуры и платформы больших данных |
| [X.1770](http://handle.itu.int/11.1002/1000/14807) | 29.10.2021 г. | Действующая | АПУ | Технические руководящие указания по безопасным многопользовательским вычислениям |
| [X.1811](http://handle.itu.int/11.1002/1000/14454) | 30.04.2021 г. | Действующая | ТПУ | Руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность |
| [Z.100 Приложение F1](http://handle.itu.int/11.1002/1000/13732) | 13.11.2018 г. | Замененная | АПУ | Язык спецификации и описания: Обзор SDL-2010 |
| [Z.100 Приложение F2](http://handle.itu.int/11.1002/1000/13733) | 13.11.2018 г. | Замененная | АПУ | Язык спецификации и описания: Обзор SDL-2010 |
| [Z.100 Приложение F3](http://handle.itu.int/11.1002/1000/13734) | 13.11.2018 г. | Замененная | АПУ | Язык спецификации и описания: Обзор SDL-2010 |
| [Z.100](http://handle.itu.int/11.1002/1000/14048) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания: Обзор SDL-2010 |
| [Z.100 Приложение F2](http://handle.itu.int/11.1002/1000/14050) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания: Обзор SDL-2010 – Формальное определение SDL‑2010: Статическая семантика |
| [Z.100 Приложение F3](http://handle.itu.int/11.1002/1000/14051) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания: Обзор SDL-2010 – Формальное определение SDL‑2010: Динамическая семантика |
| [Z.100](http://handle.itu.int/11.1002/1000/14670) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания: Обзор SDL-2010 |
| [Z.100 Приложение F1](http://handle.itu.int/11.1002/1000/14049) | 14.10.2019 г. | Действующая | АПУ | Язык спецификации и описания: Обзор SDL-2010 – Формальное определение SDL: Общий обзор |
| [Z.100 Приложение F2](http://handle.itu.int/11.1002/1000/14702) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания: Обзор SDL-2010 – Формальное определение SDL: Статическая семантика |
| [Z.100 Приложение F3](http://handle.itu.int/11.1002/1000/14703) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания: Обзор SDL-2010 – Формальное определение SDL: Динамическая семантика |
| [Z.101](http://handle.itu.int/11.1002/1000/14052) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания − Основной SDL-2010 |
| [Z.101](http://handle.itu.int/11.1002/1000/14671) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания − Основной SDL-2010 |
| [Z.102](http://handle.itu.int/11.1002/1000/14053) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания − Комплексный SDL-2010 |
| [Z.102](http://handle.itu.int/11.1002/1000/14672) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания − Комплексный SDL-2010 |
| [Z.103](http://handle.itu.int/11.1002/1000/14054) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания – Краткие нотации и аннотации в SDL-2010 |
| [Z.103](http://handle.itu.int/11.1002/1000/14673) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания – Краткие нотации и аннотации в SDL-2010 |
| [Z.104](http://handle.itu.int/11.1002/1000/14055) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания − Язык данных и действий в SDL-2010 |
| [Z.104](http://handle.itu.int/11.1002/1000/14674) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания − Язык данных и действий в SDL-2010 |
| [Z.105](http://handle.itu.int/11.1002/1000/14056) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания – Сочетание SDL-2010 с модулями ASN.1 |
| [Z.105](http://handle.itu.int/11.1002/1000/14675) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания – Сочетание SDL-2010 с модулями ASN.1 |
| [Z.106](http://handle.itu.int/11.1002/1000/14057) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания – Общий формат обмена для SDL-2010 |
| [Z.106](http://handle.itu.int/11.1002/1000/14676) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания – Общий формат обмена для SDL-2010 |
| [Z.107](http://handle.itu.int/11.1002/1000/14058) | 14.10.2019 г. | Замененная | АПУ | Язык спецификации и описания – Объектно-ориентированные данные в SDL‑2010 |
| [Z.107](http://handle.itu.int/11.1002/1000/14677) | 13.06.2021 г. | Действующая | АПУ | Язык спецификации и описания – Объектно-ориентированные данные в SDL‑2010 |
| [Z.151](http://handle.itu.int/11.1002/1000/13711) | 14.10.2018 г. | Действующая | АПУ | Нотация требований пользователя (URN) – Определение языка |
| [Z.161](http://handle.itu.int/11.1002/1000/13369) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Основной язык TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/13703) | 14.10.2018 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Основной язык TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/14059) | 14.10.2019 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Основной язык TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/14480) | 29.10.2020 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Основной язык TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/14781) | 14.10.2021 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Основной язык TTCN-3 |
| [Z.161.1](http://handle.itu.int/11.1002/1000/13370) | 14.10.2017 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Поддержка интерфейсов с постоянными сигналами |
| [Z.161.2](http://handle.itu.int/11.1002/1000/13371) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Конфигурация и поддержка развертывания |
| [Z.161.2](http://handle.itu.int/11.1002/1000/13704) | 14.10.2018 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Конфигурация и поддержка развертывания |
| [Z.161.2](http://handle.itu.int/11.1002/1000/14060) | 14.10.2019 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Конфигурация и поддержка развертывания |
| [Z.161.2](http://handle.itu.int/11.1002/1000/14782) | 14.10.2021 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Конфигурация и поддержка развертывания |
| [Z.161.3](http://handle.itu.int/11.1002/1000/13372) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Усовершенствованная параметризация |
| [Z.161.3](http://handle.itu.int/11.1002/1000/14481) | 29.10.2020 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Усовершенствованная параметризация |
| [Z.161.3](http://handle.itu.int/11.1002/1000/14783) | 14.10.2021 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Усовершенствованная параметризация |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13373) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Типы поведения |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13705) | 14.10.2018 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Типы поведения |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14482) | 29.10.2020 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Типы поведения |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14784) | 14.10.2021 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Типы поведения |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13374) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Усовершенствованное согласование |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13706) | 14.10.2018 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Усовершенствованное согласование |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14061) | 14.10.2019 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Усовершенствованное согласование |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14483) | 29.10.2020 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Усовершенствованное согласование |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14062) | 14.10.2019 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Объектно-ориентированные свойства |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14484) | 29.10.2020 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Объектно-ориентированные свойства |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14785) | 14.10.2021 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Расширения для языка TTCN-3: Объектно-ориентированные свойства |
| [Z.164](http://handle.itu.int/11.1002/1000/13375) | 14.10.2017 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Операционная семантика TTCN-3 |
| [Z.165](http://handle.itu.int/11.1002/1000/13376) | 14.10.2017 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Интерфейс времени выполнения TTCN-3 (TRI) |
| [Z.165.1](http://handle.itu.int/11.1002/1000/14485) | 29.10.2020 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Пакет расширений TTCN-3: Расширенный TRI |
| [Z.166](http://handle.itu.int/11.1002/1000/13377) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Интерфейс управления TTCN-3 (TCI) |
| [Z.166](http://handle.itu.int/11.1002/1000/13707) | 14.10.2018 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Интерфейс управления TTCN-3 (TCI) |
| [Z.166](http://handle.itu.int/11.1002/1000/14063) | 14.10.2019 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Интерфейс управления TTCN-3 (TCI) |
| [Z.166](http://handle.itu.int/11.1002/1000/14486) | 29.10.2020 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Интерфейс управления TTCN-3 (TCI) |
| [Z.167](http://handle.itu.int/11.1002/1000/13378) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование ASN.1 с TTCN-3 |
| [Z.167](http://handle.itu.int/11.1002/1000/13708) | 14.10.2018 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование ASN.1 с TTCN-3 |
| [Z.167](http://handle.itu.int/11.1002/1000/14487) | 29.10.2020 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование ASN.1 с TTCN-3 |
| [Z.167](http://handle.itu.int/11.1002/1000/14786) | 14.10.2021 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование ASN.1 с TTCN-3 |
| [Z.168](http://handle.itu.int/11.1002/1000/13379) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Преобразование языка IDL в TTCN-3 |
| [Z.168](http://handle.itu.int/11.1002/1000/14787) | 14.10.2021 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Преобразование языка IDL в TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/13380) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование схемы XML с TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/13709) | 14.10.2018 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование схемы XML с TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14064) | 14.10.2019 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование схемы XML с TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14488) | 29.10.2020 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование схемы XML с TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14788) | 14.10.2021 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование схемы XML с TTCN-3 |
| [Z.170](http://handle.itu.int/11.1002/1000/13381) | 14.10.2017 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Спецификация замечаний по документации TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/13382) | 14.10.2017 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование JSON с TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/13710) | 14.10.2018 г. | Замененная | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование JSON с TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/14789) | 14.10.2021 г. | Действующая | АПУ | Нотация для тестирования и управления тестированием версии 3: Использование JSON с TTCN-3 |

ТАБЛИЦА 8

17-я Исследовательская комиссия – Рекомендации, по которым получено согласие/сделано заключение   
и которые еще не утверждены

| Рекомендация | Сделано заключение/ получено согласие | ТПУ/ АПУ | Название |
| --- | --- | --- | --- |
| X.672 | 03.09.2021 г. | АПУ | Система разрешения идентификатора объекта |
| Поправка 1 к X.1246 | 03.09.2021 г. | ТПУ | Технологии, используемые в организациях электросвязи для противодействия голосовому спаму |
| Поправка 1 к X.1247 | 03.09.2021 г. | ТПУ | Техническая основа противодействия спаму при передаче сообщений на мобильные устройства |
| Исправление к X.1712 | 07.01.2022 г. | АПУ | Требования и меры безопасности для сетей QKD – Управление ключами |
| X.1812 (X.5Gsec-t) | 03.09.2021 | ТПУ | Структура безопасности на основе доверительных отношений для экосистемы IMT-2020 |

ТАБЛИЦА 9

17-я Исследовательская комиссия – Рекомендации, исключенные в течение исследовательского периода

| Рекомендация | Последняя по времени версия | Дата  исключения | Название |
| --- | --- | --- | --- |
| Отсутствует |  |  |  |

ТАБЛИЦА 10

17-я Исследовательская комиссия – Рекомендации, представленные на ВАСЭ-20

| Рекомендация | Предложение | Название | Ссылка |
| --- | --- | --- | --- |
| Отсутствует |  |  |  |

ТАБЛИЦА 11

17-я Исследовательская комиссия – Добавления

| Добавление | Утверждение | Статус | Название |
| --- | --- | --- | --- |
| [X Добавление 13](http://handle.itu.int/11.1002/1000/13730) | 07.09.2018 г. | Действующее | МСЭ-Т Х.1051 – Добавление по руководству для пользователей по управлению информационной безопасностью для Рекомендации МСЭ-T X.1051 |
| [X Добавление 26 (2016 г.) Испр.1](http://handle.itu.int/11.1002/1000/13592) | 29.03.2018 г. | Действующее |  |
| [X Добавление 29](http://handle.itu.int/11.1002/1000/13409) | 06.09.2017 г. | Действующее | МСЭ-T X.1242 – Добавление по руководящим указаниям по мерам противодействия атакам типа "фишинг" и "смишинг" через службу коротких сообщений |
| [X Добавление 30](http://handle.itu.int/11.1002/1000/13410) | 06.09.2017 г. | Действующее | МСЭ-T X.805 – Добавление по руководству по безопасности для оператора виртуальной сети подвижной связи |
| [X Добавление 31](http://handle.itu.int/11.1002/1000/13411) | 06.09.2017 г. | Действующее | МСЭ-T X.660 – Добавление по руководящим указаниям по использованию идентификаторов объектов для интернета вещей |
| [X Добавление 32](http://handle.itu.int/11.1002/1000/13593) | 29.03.2018 г. | Действующее | МСЭ-T X.1058 – Добавление по своду правил и норм для защиты информации, позволяющей установить личность (PII), для организаций электросвязи |
| [X Добавление 33](http://handle.itu.int/11.1002/1000/13731) | 07.09.2018 г. | Действующее | МСЭ-T X.1231 – Добавление по технической основе для противодействия мошенничеству в телефонных услугах |
| [X Добавление 34](http://handle.itu.int/11.1002/1000/13869) | 30.01.2019 г. | Действующее | МСЭ-T X.1051 – Добавление по руководящим указаниям по управлению информационной безопасностью для организаций электросвязи |
| [X Добавление 35](http://handle.itu.int/11.1002/1000/14066) | 05.09.2019 г. | Действующее | МСЭ-T X.1254 – Добавление по сценариям использования структуры гарантии аутентификации объекта (EAA) |
| [X Добавление 36](http://handle.itu.int/11.1002/1000/14809) | 03.09.2021 г. | Действующее | МСЭ-T X.1051 – Добавление по важнейшим мерам по обеспечению безопасности для управления информационной и сетевой безопасностью организаций электросвязи |

ТАБЛИЦА 12

17-я Исследовательская комиссия – Согласованные ненормативные публикации   
(Справочники, Руководства)

| Обозначение | Дата | Название | Тип публикации |
| --- | --- | --- | --- |
| [TP.inno](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15153) | 03.09.2020 г. | Описание механизма инкубации и способов его улучшения | Технический документ |
| [TP.sgstruct](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15154) | 03.09.2020 г. | Стратегические подходы к преобразованию исследований в области безопасности | Технический документ |
| [TR.ors](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15256) | 26.03.2020 г. | Система разрешения для OID: Проблемы, требования и возможные решения | Технический отчет |
| [TR.sec-manual](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14367) | 03.09.2020 г. | Безопасность в электросвязи и информационных технологиях (седьмое издание) | Технический отчет |
| [TR.sec-qkd](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14825) | 26.03.2020 г. | Соображения безопасности в отношении сети с поддержкой квантового распределения ключей | Технический отчет |
| [TR.Suss](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14370) | 03.09.2020 г. | Эффективное использование стандартов безопасности (второе издание) | Технический отчет |
| [TR.usm](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15241) | 03.09.2020 г. | Унифицированная модель безопасности (USM) – нейтральный интегрированный системный подход к кибербезопасности | Технический отчет |
| [TR.XAASL](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16769) | 03.09.2021 г. | Технический отчет: Структура стандартизации безопасности для виртуализированных услуг | Технический отчет |
| [XSTR-SEC-QKD Cor.1](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16969) | 30.04.2021 г. | Соображения безопасности в отношении сети с поддержкой квантового распределения ключей – Исправление 1 | Технический отчет |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16983) | 30.04.2021 г. | Руководство пользователя Рекомендаций по языку спецификации и описания Z.100, версия4.0.1 | Руководство пользователя Рекомендаций |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14424) | 07.09.2018 г. | Руководство пользователя Рекомендаций по языку спецификации и описания Z.100, версия 3.0.2 | Руководство пользователя Рекомендаций |
| [Z.Imp100rev](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14816) | 05.09.2019 г. | Руководство пользователя Рекомендаций по языку спецификации и описания Z.100, версия 4.0.0 | Руководство пользователя Рекомендаций |

ТАБЛИЦА 13

17-я Исследовательская комиссия – Рекомендации, по которым сделано заключение/получено согласие   
и которые отклонены

| Рекомендация | Сделано заключение/ получено согласие | АПУ/ТПУ | Название |
| --- | --- | --- | --- |
| Отсутствует |  |  |  |

ПРИЛОЖЕНИЕ 2

**Предлагаемый пересмотр к Резолюции 2 ВАСЭ**

Приложение A

ЧАСТЬ 1 – Основные области исследований

17-я Исследовательская комиссия МСЭ-Т

Безопасность

17-я Исследовательская комиссия МСЭ-Т отвечает за формирование доверия и обеспечение безопасности при использовании информационно‑коммуникационных технологий (ИКТ).

Основные области исследований 17-й Исследовательской комиссии составляют обеспечение безопасности с помощью ИКТ и обеспечение безопасности ИКТ. Сюда относится проведение исследований по вопросам кибербезопасности, внешних услуг по обеспечению безопасности, обнаружения угроз и реакции на конечных точках, управления безопасностью, противодействия спаму и управления определением идентичности. Сюда относятся также вопросы архитектуры и структуры безопасности, квантовой безопасности, безопасности технологии распределенного реестра (DLT), безопасности интеллектуальных транспортных систем, аспекты безопасности, связанные с ИИ, а также вопросы безопасности сетей, приложений и услуг, таких как интернет вещей (IoT) и "умные" города, различные виды сетей, включая IMT2020/5G и далее, "умные" электросети, система управления технологическими процессами (ICS), цепочка поставок, смартфоны, организация сетей с программируемыми параметрами (SDN), виртуализация сетевых функций (NFV), телевидение на основе протокола Интернет (IPTV), веб‑услуги, over-the-top (OTT), социальные сети, облачные вычисления, анализ больших данных, цифровая финансовая система и телебиометрия.

Укрепление доверия и безопасности при использовании ИКТ также включает защиту информации, позволяющей установить личность (PII), например технические и эксплуатационные аспекты защиты данных в части обеспечения конфиденциальности, целостности и доступности PII.

17‑я Исследовательская комиссия также отвечает за приложения открытых систем связи, в том числе каталоги и идентификаторы объектов, за технические языки, метод их использования и другие вопросы, относящиеся к аспектам программного обеспечения систем электросвязи, и за языки спецификации тестирования для поддержки проверки на соответствие в целях повышения качества Рекомендаций.

ЧАСТЬ 2 – Ведущие исследовательские комиссии МСЭ-Т в конкретных областях исследований

ИК17 Ведущая исследовательская комиссия по вопросам безопасности  
Ведущая исследовательская комиссия по вопросам управления определением идентичности  
Ведущая исследовательская комиссия по вопросам языков и методов описания

Приложение В   
(к Резолюции 2 ВАСЭ)

Руководящие ориентиры для исследовательских комиссий МСЭ-Т  
по составлению программы работы после 2020 года

17-я Исследовательская комиссия МСЭ-Т

17-я Исследовательская комиссия МСЭ-Т отвечает за разработку ключевых технических Рекомендаций, обеспечивающих формирование доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ).

В связи с этим сюда относится проведение исследований по вопросам безопасности, включая кибербезопасность, противодействие спаму и управление определением идентичности. Сюда относятся также вопросы архитектуры и структуры безопасности, управления безопасностью, а также вопросы безопасности сетей, приложений и услуг, таких как интернет вещей (IoT), интеллектуальная транспортная система, безопасные прикладные услуги, социальные сети, облачные вычисления, технология распределенного реестра и телебиометрия. 17‑я Исследовательская комиссия также отвечает за вопросы применения открытых систем связи, включая каталог и идентификаторы объектов, за технические языки, методы их использования и другие вопросы, связанные с аспектами программного обеспечения систем электросвязи, а также за проверку на соответствие в целях повышения качества Рекомендаций.

Роль 17-й Исследовательской комиссии МСЭ-Т заключается в предоставлении технических решений для обеспечения безопасности ИКТ и обеспечения безопасности с помощью ИКТ. Особое внимание уделяется, в частности, исследованиям по вопросам безопасности в новых возникающих областях, таких как безопасность IMT‑2020/5G и далее, интернет вещей (IoT), "умные" города, технологии распределенного реестра (DLT), анализ больших данных, интеллектуальная транспортная система, аспекты безопасности, связанные с ИИ, и квантовые технологии. Области исследования также включают управление информацией, позволяющей установить личность (PII), например технические и эксплуатационные аспекты защиты данных в части обеспечения конфиденциальности, целостности и доступности PII.

В области безопасности 17-я Исследовательская комиссия отвечает за разработку основных Рекомендаций по таким вопросам безопасности ИКТ, как архитектура и структуры безопасности; основы, касающиеся кибербезопасности, включая угрозы, уязвимости и риски, реагирование/реакция на инциденты и цифровую техническую экспертизу; управление безопасностью, включая управление PII, например технические и эксплуатационные аспекты защиты данных; а также борьба со спамом техническими средствами.

17‑я Исследовательская комиссия обеспечивает общую координацию деятельности в области безопасности в рамках МСЭ-Т, являясь ведущей исследовательской комиссией по вопросам безопасности, управления определением идентичности, а также языков и методов описания.

Наряду с этим 17-я Исследовательская комиссия отвечает за разработку основных Рекомендаций по безопасности технологий распределенного реестра, безопасности интеллектуальной транспортной системы, аспектам безопасности приложений и услуг в области IPTV, различных видов сетей, включая IMT-2020/5G и далее, "умных" электросетей, системы управления технологическими процессами (ICS), цепочек поставок, IoT, SDN, NFV, социальных сетей, облачных вычислений, анализа больших данных, смартфонов, цифровой финансовой системы и телебиометрии.

17-я Исследовательская комиссия отвечает также за разработку основных Рекомендаций по общей модели управления идентичностью, которая не зависит от сетевых технологий и поддерживает безопасный обмен информацией об идентичности между объектами. Эта работа также включает в себя исследование процесса обнаружения авторитетных источников информации об идентичности; общих механизмов для соединения/функционального взаимодействия различных наборов форматов информации об идентичности; угроз управлению определением идентичности; механизмов противодействия этим угрозам; защиты информации, позволяющей установить личность (PII); а также разработку механизмов обеспечения того, чтобы доступ к PII был разрешен только в случае необходимости.

В том что касается открытых систем связи, 17-я Исследовательская комиссия отвечает за Рекомендации в следующих областях:

• справочные службы и системы, включая инфраструктуру открытых ключей (PKI) (серии МСЭ‑Т F.500 и МСЭ-Т Х.500);

• идентификаторы объектов (OID) и связанные с ними органы регистрации (серии МСЭ‑Т X.660/МСЭ-Т X.670);

• взаимосвязь открытых систем (OSI), включая абстрактную синтаксическую нотацию версии 1 (ASN.1) (серии МСЭ-Т F.400, МСЭ-Т X.200, МСЭ-Т X.400, МСЭ-Т X.600, МСЭ‑Т X.800); и

• открытая распределенная обработка (ODP) (серии МСЭ-Т Х.900).

В области языков 17-я Исследовательская комиссия отвечает за проведение исследований, касающихся методов моделирования, спецификации и описания, которые включают такие языки, как ASN.1, SDL, MSC, URN и TTCN-3.

17-я Исследовательская комиссия координирует работу всех исследовательских комиссий МСЭ-Т, относящуюся к безопасности. Эта работа будет проводиться в соответствии с потребностями соответствующих исследовательских комиссий, таких как 2-я, 9-я, 11-я, 13-я, 15-я и 16‑я Исследовательские комиссии и 20‑я Исследовательская комиссия и в сотрудничестве с ними.

17-я Исследовательская комиссия будет работать над соответствующими аспектами управления определением идентичности в сотрудничестве с 20-й Исследовательской комиссией и 2‑й Исследовательской комиссией согласно мандату каждой исследовательской комиссии.

Приложение С  
(к Резолюции 2 ВАСЭ)

Перечень Рекомендаций, входящих в сферу ответственности   
соответствующих исследовательских комиссий и КГСЭ   
на исследовательский период 2021−2024 годов

…

17-я Исследовательская комиссия МСЭ-Т

МСЭ-Т E.104, МСЭ-Т E.115, МСЭ-Т E.409 (совместно с 2-й Исследовательской комиссией)

Серия МСЭ-Т F.400; МСЭ-Т F.500 – МСЭ-Т F.549

Серия МСЭ-Т Х, за исключением тех Рекомендаций, которые входят в сферу ответственности 2-й, 3‑й, 11‑й, 13-й, 15-й и 16‑й Исследовательских комиссий

Серия МСЭ-Т Z, за исключением серий МСЭ-T Z.300 и МСЭ-T Z.500

…

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