|  |  |
| --- | --- |
| **СОВЕТ 2020Женева, 9–19 июня 2020 года** |  |
|  |  |
|  |  |
| **Пункт повестки дня: PL 1.4** | **Документ C20/18-R** |
| **30 марта 2020 года** |
| **Оригинал: английский** |
| Отчет Генерального секретаря |
| ВИДЫ ДЕЯТЕЛЬНОСТИ МСЭ ПО УСИЛЕНИЮ РОЛИ МСЭ В УКРЕПЛЕНИИ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ |

|  |
| --- |
| РезюмеВ настоящем отчете кратко представлены виды деятельности МСЭ, которые осуществлялись после сессии Совета 2019 года в связи с Резолюцией 130 (Пересм. Дубай, 2018 г.), роль МСЭ как единственной содействующей организации по Направлению деятельности С5 ВВУИО, а также другие решения Членов МСЭ по усилению роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ).Необходимые действияСовету предлагается **принять к сведению** настоящий отчет.\_\_\_\_\_\_\_\_\_\_\_\_Справочные материалы*Резолюции* [*71*](https://www.itu.int/en/council/Documents/basic-texts/RES-071-R.pdf)*,* [*130*](https://www.itu.int/en/council/Documents/basic-texts/RES-130-R.pdf)*,* [*140*](https://www.itu.int/en/council/Documents/basic-texts/RES-140-R.pdf)*,* [*174*](https://www.itu.int/en/council/Documents/basic-texts/RES-174-R.pdf), [*179*](https://www.itu.int/en/council/Documents/basic-texts/RES-179-R.pdf) *(Пересм. Дубай, 2018 г.),* [*181*](http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf) *(Гвадалахара, 2010 г.) Полномочной конференции,* [*РМЭ*](http://www.itu.int/pub/S-CONF-WCIT-2012/en) *(Пересм. Дубай, 2012 г.),* [*Резолюция 1306*](https://www.itu.int/md/S15-CL-C-0109/en) *Совета, Резолюции* [*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf) *(Пересм. Дубай, 2014 г.),* [*2, 67, 69* *(Пересм. Буэнос-Айрес, 2017 г.)*](https://www.itu.int/md/D14-WTDC17-C-0115/en) *ВКРЭ, Задача 2/Конечный результат 2.2 МСЭ-D (*[*План действий Буэнос-Айреса*](https://www.itu.int/md/D14-WTDC17-C-0115/en)*), Резолюции* [*50*](https://www.itu.int/pub/T-RES-T.50-2016)*,* [*52*](https://www.itu.int/pub/T-RES-T.52-2016)*,* [*75*](https://www.itu.int/pub/T-RES-T.75-2016) *(Пересм. Хаммамет, 2016 г.),* [*58*](https://www.itu.int/pub/T-RES-T.58-2016) *(Пересм. Дубай, 2012 г.) ВАСЭ, Документы [C15/18](http://www.itu.int/md/S15-CL-C-0018/en),* [*C16/18*](https://www.itu.int/md/S16-CL-C-0018/en)*,* [*C17/18*](https://www.itu.int/md/S17-CL-C-0018/en)*,* [*C18/18*](https://www.itu.int/md/S18-CL-C-0018/en)*,* [*C19/18*](https://www.itu.int/md/S19-CL-C-0018/en) *Совета* |

# 1 Виды деятельности в области кибербезопасности и противодействия спаму

1.1 Развитие ИКТ, основу которого составляют безопасность и доверие, признано важнейшим фактором устойчивого развития. Настоящий отчет, построенный на базе пяти основных составляющих Глобальной программы кибербезопасности (ГПК), отражает взаимодополняющий характер существующих программ работы МСЭ и способствует реализации различных видов деятельности БРЭ, БСЭ и БР в этой области.

**2 Меры правового характера**

2.1 В рамках Задачи 2/Конечного результата 2.2 Плана действий Буэнос-Айреса и с учетом Вопроса 3/2 ИК2 МСЭ‑D (ранее Вопрос 22/1) МСЭ оказывает помощь Государствам-Членам в понимании ими правовых аспектов кибербезопасности, используя для этого [ресурсы МСЭ по законодательству в области киберпреступности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx), с тем чтобы помочь в согласовании их нормативно-правовых баз. В области правовых мер МСЭ тесно сотрудничает с такими партнерами, как УНП ООН, и с другими экспертами.

**3 Технические и процедурные меры**

3.1 [ИК17](http://www.itu.int/ITU-T/studygroups/com17/) МСЭ-Т, ведущая исследовательская комиссия по вопросам безопасности и по вопросам управления определением идентичности (IdM), по-прежнему играет важную роль в проведении исследований и стандартизации в области кибербезопасности, борьбы со спамом, IdM, сертификатов X.509 МСЭ-Т, управления информационной безопасностью, повсеместно распространенных сенсорных сетей, телебиометрии, безопасности подвижной связи, безопасности виртуализации в интересах безопасности облачных вычислений, защиты информации, позволяющей установить личность, а также архитектуры безопасности и безопасности приложений, в сотрудничестве с внешними организациями по разработке стандартов.

3.2 Со времени последнего отчета Совету ИК17 провела одно собрание в сентябре 2019 года, на котором ИК17 создала [25 новых направлений работы по стандартизации](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). ИК17 утвердила более 30 новых или пересмотренных Рекомендаций МСЭ-Т по безопасности в области ИКТ, а именно: 9‑е издание основных стандартов по кибербезопасности серии Рекомендаций X.500 по инфраструктуре открытых ключей, X.1044 "Требования безопасности виртуализации сетей", X.1045 "Архитектура цепочки услуг безопасности для сетей и приложений", X.1059 "Руководство по внедрению в организациях электросвязи управления рисками в отношении своих активов, доступных по глобальным сетям на базе IP", X.1702 "Архитектура генератора случайных чисел квантового шума", X.1232 "Техническая основа противодействия рекламному спаму в информации, генерируемой пользователями", X.677 "Механизм идентификации для беспилотных летательных аппаратов, использующих идентификаторы объектов", X.1402 "Угрозы безопасности технологии распределенного реестра", Поправка 1 X.1197 "Руководящие указания по критериям выбора криптографических алгоритмов для услуг IPTV и защиты контента", Испр. 1 X.694 и Испр. 1 X.893 по ASN.1, пересмотренная серия Z.100 по ЦАЛ и пересмотренная серия Z.160 по нотации для тестирования и управления тестированием версии 3 (TTCN-3). ИК17 также утвердила новое Добавление по сценариям использования структуры гарантии аутентификации объекта (EAA) и пересмотренное руководство пользователя серии Z.

3.3 ИК17 провела однодневный [семинар-практикум МСЭ по безопасности финансовых технологий](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190826/Pages/default.aspx) 26 августа 2019 года, на котором были выдвинуты предложения по последующей деятельности ИК17 в сотрудничестве с другими определенными организациями по разработке стандартов, связанными с безопасностью финансовых технологий, т. е. ОГ-DLT, ОГ-DFC, ТК 307 ИСО, W3C по DLT. ИК17 также провела [минисеминар-практикум по проблемам кибербезопасности при автоматическом вождении](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx) 26 августа 2019 года совместно с Сотрудничеством МСЭ по стандартам связи для ИТС (CITS) и РГ29 ЕЭК ООН.

3.4 Ввиду распространения по всему миру коронавирусной инфекции собрание ИК17, проведенное 17–26 марта 2020 года, стало первым полностью виртуальным собранием исследовательской комиссии МСЭ-Т. Также ИК17 пришлось отложить проведение [совместного семинара-практикума ИК17 МСЭ-Т и ТК 307 ИСО "Безопасность, управление определением идентичности и конфиденциальность](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20200316/Pages/default.aspx)", планировавшееся на 16 марта 2020 года.

3.5 ИК17 продолжила работу по безопасности IoT и осуществляла координацию с ИК20 МСЭ-Т "IoT и его приложения, включая "умные" города и сообщества (SC&C)".

3.6 ИК9 МСЭ-Т сделала заключения по пяти проектам Рекомендаций МСЭ-Т: J.1012 J.1013, J.1014, J.1015 и J.1015.1 по встроенному общему интерфейсу для заменяемых решений CA/DRM.

3.7 ИК13 МСЭ-Т утвердила Рекомендацию МСЭ-Т Y.3053 (2018 г.) − Поправка 1 "Принципы организации надежных сетей с сетевыми доменами, ориентированными на доверие: Поправка 1 – Архитектура и процедуры развертывания при организации надежных сетей", Y.3514 − Исправление 1 "Облачные вычисления – Структура и требования для доверенных межоблачных вычислений" и Y.3517 "Облачные вычисления – Обзор управления межоблачным доверием".

3.8 ИК15 МСЭ-Т проводит работу по Добавлению (G.Sup.otnsec), в котором описываются язык и общая инфраструктура данных в существующих уровнях протокола оптической транспортной сети (ОТС), которые требуются для использования предложенных в независимом порядке криптографических протоколов с целью создания защищенных транспортных решений на выбранных уровнях ОТС.

3.9 ИК20 МСЭ-Т утвердила Рекомендацию МСЭ-Т Y.4807 "Обеспечиваемая проектным решением гибкость безопасности систем электросвязи/ИКТ в интернете вещей".

3.10 Несколько оперативных групп МСЭ-Т изучают в рамках своей работы аспект доверия к различным возникающим технологиям. К их числу относятся: 1) [*Оперативная группа МСЭ-Т по машинному обучению для будущих сетей, включая 5G (ОГ-ML5G)*](https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx), 2) [*Оперативная группа МСЭ-Т "Технологии для Сети-2030 (ОГ-NET-2030)*](https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx), 3) [*Оперативная группа МСЭ-T по искусственному интеллекту для здравоохранения (ОГ-AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h), 4) [*Оперативная группа МСЭ-Т по мультимедиа в автотранспортных средствах (ОГ-VM)*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx), 5) [*Оперативная группа МСЭ-Т "ИИ для автономного и ассистированного вождения" (ОГ-AI4AD)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx), 6) [*Оперативная группа МСЭ-Т по квантовым информационным технологиям для сетей (ОГ-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx).

3.11 МСЭ совместно с Фондом Билла и Мелинды Гейтс, Группой Всемирного банка и Банком международных расчетов провел семинар-практикум по безопасности, инфраструктуре и доверию для цифровых финансовых услуг, который состоялся 4–5 декабря 2019 года в штаб-квартире МСЭ в Женеве, Швейцария.

3.12 Продолжается работа МСЭ-R по стандартизации в области радиосвязи с учетом постоянного развития современных сетей электросвязи. МСЭ-R разработал четкие принципы безопасности для сетей IMT (3G, 4G и 5G) (Рекомендации МСЭ-R M.1078, M.1223, M.1457, M.1645, М.2012 и М.2083). Выпущены также Рекомендации по вопросам безопасности в архитектуре сетевого управления для цифровых спутниковых систем (Рекомендация МСЭ-R S.1250) и по повышению производительности протокола управления передачей по спутниковым сетям (Рекомендация МСЭ-R S.1711).

**4 Организационные структуры**

4.1 МСЭ провел технические оценки готовности к созданию групп реагирования на компьютерные инциденты (CIRT) в 76 странах и проводит необходимые последующие действия. Завершено непосредственное участие в 14 таких мероприятиях. В ходе оказания услуг CIRT и осуществления связанного с этим проекта по созданию потенциала Государству Палестина была оказана помощь в создании и развертывании технического потенциала и связанных с этим учебных занятиях по деятельности CIRT. Помощь в разработке национальных стратегий кибербезопасности получили Кирибати и Соломоновы Острова. Помощь в наращивании потенциала для CIRT была оказана Папуа-Новой Гвинее и Вануату в рамках [проекта МСЭ и Министерства связи и искусств (DoCA) Австралии](https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9RAS18061). Семинары-практикумы по обеспечению готовности к созданию CIRT были проведены в Чаде и Либерии. Заинтересованные стороны CIRT национального уровня в Гамбии прошли профессиональную подготовку по деятельности CIRT. Было начато осуществление четырех проектов CIRT, которое продолжается в Ботсване, Бурунди, Гамбии и Малави. В Кении продолжается совершенствование существующих CIRT (должно быть завершено в 2020 г.).

4.2 МСЭ провел 28 [тренировочных занятий по кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), в которых участвовали свыше 100 стран. Тренировочные занятия по кибербезопасности прошли в: [Уганде](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Africa-Cyberdrill-2019.aspx) (Африканский регион, ноябрь 2019 г.); [Омане](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx)(Арабский регион, октябрь 2019 г.); [Малайзии](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/ASP-CIS-Cyberdrill-2019.aspx) (Азиатско-Тихоокеанский регион, сентябрь 2019 г.); и Румынии (регион СНГ и Европы, май 2019 г.). В 2020 году планируется провести пять тренировочных занятий по кибербезопасности.

**5 Создание потенциала**

5.1 МСЭ провел для всех регионов МСЭ [региональные форумы по кибербезопасности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) с целью создания потенциала для различных программ и видов деятельности БРЭ, а также обеспечения рабочей платформы для сотрудничества на региональном и международном уровнях.

5.2После ВКРЭ 2017 года, в течение исследовательского периода 2018−2021 годов, продолжится работа по Вопросу 3/2 ИК2 МСЭ-D ([Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности](http://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=1&sp=2014&rgq=D14-SG02-RGQ03.2&stg=2)).

5.3 Руководство МСЭ по разработке национальной стратегии кибербезопасности (NCS) является руководством на основе примеров передового опыта, которое используется странами всех регионов. В 2019 году были проведены следующие семинары-практикумы: a) региональный семинар-практикум , который принимали Министерство информатики и Агентство кибербезопасности Индонезии в Джакарте, по стратегиям кибербезопасности (в том числе обсуждались общие нормы защиты данных); b) региональный семинар-практикум , который принимала Македония, по совершенствованию национальных стратегий для пяти балканских государств; c) региональный семинар-практикум , который принимал Тунис, по совершенствованию национальных стратегий стран регионов Африки и арабских государств. Активное участие принимали 20 стран. Три страны получили прямую помощь по разработке и пересмотру национальных стратегий кибербезопасности с использованием этого руководства.

5.4 Судану оказана техническая помощь и помощь по развитию потенциала в целях совершенствования государственной стратегии защиты важнейшей информационной инфраструктуры.

5.5 В ходе Региональной недели кибербезопасности для региона арабских государств Арабский региональный центр кибербезопасности МСЭ (МСЭ-ARCC) способствовал обмену информацией и созданию потенциала в области кибербезопасности. Неделя предоставила платформу, позволившую старшим должностным лицам в области ИКТ и кибербезопасности в регионе встретиться с соответствующими заинтересованными сторонами и обсудить угрозы, эволюцию, возможности и проблемы кибербезопасности.

5.6 В Кишиневе (Молдова) при поддержке МСЭ прошла неделя кибербезопасности Молдовы. Конференция предоставила возможности для общения и платформу для обмена идеями, обсуждения и совместной работы в целях развития путем инноваций, глобальных стратегий и решений в области кибербезопасности.

5.7 В Анкаре (Турция) при поддержке МСЭ проведены учения "Киберщит-2019". Основными задачами были расширение возможностей реагирования на инциденты и повышение уровня готовности, улучшение взаимопонимания в отношении киберрисков и их последствий, а также обеспечение продолжения совместной деятельности международных заинтересованных сторон в области кибербезопасности, особенно национальных CIRT, в целях предотвращения киберугроз. МСЭ также провел для Кыргызстана сессию профессиональной подготовки по созданию центра операций в области кибербезопасности.

5.8 МСЭ, Центр повышения квалификации в области электросвязи и Факультет прикладных наук почты и электросвязи (Факультет ИКТ, Исламская Республика Иран) провели [профессиональную подготовку по кибербезопасности ЦПМ АТР МСЭ](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2018/CybersecurityASPCOE/cybersecurity.aspx) (Тегеран, Иран – декабрь 2018 г.).

5.9 Третья итерация [Глобального индекса кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) показывает значительное совершенствование приверженности кибербезопасности во всем мире. Было проведено в четвертый раз обследование по линии Глобального индекса кибербезопасности, с улучшенными вопросником и методикой. В партнерстве с компанией Deloitte в Кот-д'Ивуаре был проведен анализ положения в области кибербезопасности, в том числе по результатам GCI. Анализ помог стране определить первоочередные инициативы в области кибербезопасности для улучшения положения в этой сфере.

**6 Международное сотрудничество**

6.1 МСЭ развивает отношения и [партнерские связи](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) с различными региональными/международными организациями и инициативами, в том числе с Инициативой Содружества по борьбе с киберпреступностью, ENISA, Интерполом, ЭКОВАС, Всемирным банком, FIRST и региональными ассоциациями CSIRT/CERT, такими как AP CERT, AFRICA CERT и OIC CERT.

6.2 По просьбе Саудовской Аравии как председателя Группы 20 МСЭ оказывает ей поддержку в качестве партнера в области знаний по различным направлениям, включая приоритет безопасности в цифровой экономике, в рамках деятельности с участием многих заинтересованных сторон, проводимой секретариатом Группы 20 с привлечением соответствующих международных организаций.

6.3 Как ведущая содействующая организация по Направлению деятельности  C5 ВВУИО МСЭ организовал несколько сессий [Форума ВВУИО 2019 года](https://www.itu.int/net4/wsis/forum/2019/), в том числе сессию высокого уровня по ИИ и доверию, а также сессию по значению измерения кибербезопасности.

6.4 По поручению сессии Совета 2019 года Генеральный секретарь представил сессии Совета 2020 года: 1) отчет, в котором объясняется, как МСЭ в настоящее время использует систему ГПК; и 2)  разработанные при участии Государств-Членов руководящие указания по использованию ГПК МСЭ для рассмотрения и утверждения Советом.

**7 Защита ребенка в онлайновой среде (COP)**

7.1 Многосторонняя группа экспертов, в состав которой входят более 50 организаций и отдельных специалистов, приступила к пересмотру [Руководящих указаний по защите ребенка в онлайновой среде](https://www.itu.int/en/cop/Pages/guidelines.aspx), впервые изданных в 2009 году.

7.2 В Африке начались дискуссии с участием представителей Чада, Кении, Малави и Руанды о реализации основ национальной стратегии. В частности, на региональном форуме COP в Гане собрался широкий круг экспертов, чтобы провести анализ возможных решений и необходимых мер. В Азиатско-Тихоокеанского регионе была оказана помощь в разработке Региональной платформы АСЕАН по защите ребенка в онлайновой среде, основанной на Руководящих принципах COP, в координации с другими партнерами, включая TELSOM/TELMIN. Другие мероприятия проводились в Европе в рамках региональной инициативы по укреплению доверия и уверенности при использовании ИКТ.

7.3 МСЭ также выполняет функции секретариата Комиссии по широкополосной связи в интересах устойчивого развития. В Нью-Йорке в октябре 2019 года Рабочая группа по безопасности ребенка в онлайновой среде, возглавляемая Всемирным фондом детства и компанией Zain, выпустила всеобъемлющий [отчет](https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf). В качестве справочного материала в отчет были включены Руководящие принципы по СОР, которые послужили основой для выполнения рекомендаций, изложенных в отчете.

7.4 Проект регионального обзора национальных подходов к обеспечению безопасности молодежи и детей в онлайновой среде был подготовлен к ознакомлению и открыт для консультаций со странами. Также была оказана помощь Грузии и Украине в разработке национальных стратегий защиты ребенка в онлайновой среде.

7.5 В День более безопасного интернета 2020 года МСЭ провел различные мероприятия, включая популяризацию защиты детей в онлайновой среде. По случаю этого Дня был представлен новый талисман COP; его [история и базовая информация](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) о нем были придуманы и подготовлены детьми в начале января 2020 года.

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