|  |  |
| --- | --- |
| **СОВЕТ 2021 Виртуальные консультации Советников, 8–18 июня 2021 года** |  |
|  |  |
|  |  |
| **Пункт повестки дня: PL 1.4** | **Документ C21/18-R** |
| **22 февраля 2021 года** |
| **Оригинал: английский** |
| Отчет Генерального секретаря | |
| ВИДЫ ДЕЯТЕЛЬНОСТИ МСЭ ПО УСИЛЕНИЮ РОЛИ МСЭ  В УКРЕПЛЕНИИ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ  ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ | |

|  |
| --- |
| Резюме  В настоящем отчете кратко представлены виды деятельности МСЭ, которые осуществлялись в 2020 году 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).  Вариант настоящего отчета (C20/18) за 2020 год был подготовлен для представления на сессии Совета 2020 года, но не рассматривался.  Необходимые действия  Совету предлагается **принять к сведению** настоящий отчет и Документ С20/18.  \_\_\_\_\_\_\_\_\_\_\_\_  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](https://www.itu.int/md/D14-WTDC17-C-0115/en)**[(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) *и* [*C20/18*](https://www.itu.int/md/S20-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 2.2 Плана действий Буэнос-Айреса и с учетом Вопроса 3/2 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 соответствующими организациями, оказывающими помощь Государствам-Членам.

# 3 Технические и процедурные меры

3.1 [17](http://www.itu.int/ITU-T/studygroups/com17/)-я Исследовательская комиссия МСЭ-Т (ИК17), 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 2020 года, на котором ИК17 создала [15 новых направлений работы по стандартизации](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17), а также электронное пленарное заседание 7 января 2021 года. ИК17 утвердила более 40 новых или пересмотренных Рекомендаций МСЭ-Т по безопасности в области ИКТ, а именно: [X.510 | ISO/IEC 9594-11](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14320); серии [X.680−690](https://www.itu.int/rec/T-REC-x/en); [X.1046](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1046); [X.1052 (пересмотрена)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14044) и [X.1054 (пересмотрена, на этапе утверждения)](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1054); [X.1148](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14249); [X.1149](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14250); [X.1216](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14259), [X.1217](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1217)и[X.1218](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14444); [X.1254 (пересмотрена)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14260), [X.1279](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14261), [D.1140/X.1261](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1261), [X.1451](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14252) и [X.1452](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14451); [X.1363](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14087), [X.1364](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14088), [X.1365](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14089), [X.1366](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14262), [X.1367](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14263), и [X.1368](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1368)**;** [X.1371](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14090), [X.1374](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14446), [X.1375](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14447) и [X.1376](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1376), [X.1400](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14449), [X.1401](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14092), [X.1402](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14251), [X.1403](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14264) и [X.1404](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14450), [X.1606](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14265); [X.1710](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14452) и [X.1714](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14453); [X.1750](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14266) и [X.1751](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14267), иX.1811 (на этапе утверждения).

3.3 ИК17 также согласовала следующие технические отчеты: "Структура безопасности квантового распределения ключей в сетях электросвязи", "Проблемы, требования и потенциальные решения для преобразования на основе OID", "Безопасность в электросвязи и информационных технологиях (7-е издание)", "Эффективное использование стандартов безопасности (2-е издание)", "Описание механизма инкубации и способы его совершенствования", "Стратегические подходы к трансформации исследований в области безопасности", "Единая модель безопасности (USM) – нейтральный интегрированный системный подход к кибербезопасности".

3.4 В рамках подготовки к ВАСЭ-20 ИК17 приняла решение о преобразовании существующих 14 Вопросов в 12 Вопросов. В связи с переносом сроков проведения ВАСЭ-20 этот новый набор из 12 Вопросов был одобрен на собрании КГСЭ в январе 2021 года и вступил в силу 18 января 2021 года до конца исследовательского периода.

3.5 ИК3 МСЭ-T продолжает исследования экономических и политических аспектов больших данных и цифровой идентичности, относящихся к услугам международной электросвязи, в рамках Вопроса 11/3. ИК3 недавно утвердила [Рекомендацию МСЭ-T D.267/X.1261](https://www.itu.int/rec/T-REC-D.1140-202008-I).

3.6 ИК11 МСЭ-T продолжает заниматься проблематикой совершенствования протоколов сигнализации на предмет повышения их защищенности, включая разработку дополнительных требований к обмену сигнальными сообщениями и отдельных протоколов. ИК11 МСЭ-T подготовила [технический отчет QSTR-SS7-DFS](https://www.itu.int/pub/publications.aspx?lang=en&parent=T-TUT-PROTO-2019), пересмотрела стека протоколов SS7 (Q.731.3-Q.731.6) и утвердила Рекомендацию МСЭ-T [Q.3057](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.3057). Помимо этого, ИК11 МСЭ-T продолжает разработку стандартов МСЭ-Т [Q.5050](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5050), [Q.5051](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5051), [Q.5052](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5052) и [Q.5053](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5053), касающихся борьбы с контрафактными и похищенными устройствами электросвязи/ИКТ.

3.7 ИК9 МСЭ-T утвердила следующие Рекомендации, касающиеся безопасности: МСЭ-Т [J.1012](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13573), [J.1013](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13574), [J.1014](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13575), [J.1015](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13576) и [J.1015.1](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13837); МСЭ-Т [J.1204](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14357); и [J.1031](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14280), [J.1032](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14355) и [J.1033](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14356). ИК9 также утвердила три Добавления к следующим Рекомендациям серии J (МСЭ-T J.1012−J.1015.1), а именно ([J.Sup7](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14286), [J.Sup8](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14287) и [J.Sup9](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14288)).

3.8 ИК13 МСЭ-T утвердила следующие Рекомендации: МСЭ-Т [Y.3055](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14393) об основанном на доверии управлении личными данными и МСЭ-Т [Y.3801](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14258), [Y.3802](https://www.itu.int/rec/T-REC-y/recommendation.asp?lang=en&parent=T-REC-Y.3802), [Y.3803](https://www.itu.int/rec/T-REC-y/recommendation.asp?lang=en&parent=T-REC-Y.3803) и [Y.3804](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14409) о сетях квантового распределения ключей.

3.9 ИК20 МСЭ-T были разработаны следующие Рекомендации, касающиеся безопасности: [Y.4560](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14379), [Y.4561](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14380), [Y.4808](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14381) и [Y.4907](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14382).

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-T по искусственному интеллекту для здравоохранения (ОГ-AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h), 2) [*Оперативная группа МСЭ-Т по мультимедиа в автотранспортных средствах (ОГ-VM)*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx), 3) [*Оперативная группа МСЭ-Т по ИИ для автономного и ассистированного вождения (ОГ-AI4AD)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx), 4) [*Оперативная группа МСЭ-Т по квантовым информационным технологиям для сетей (ОГ-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx), 5) [*Оперативная группа МСЭ-T по ИИ в управлении операциями в случае стихийных бедствий (ОГ-AI4NDM)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx)и 6)[*Оперативная группа МСЭ-по автономным сетям (ОГ-AN)*](https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx).

3.11 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). Информация о [будущих системах подвижной связи "IMT на период до 2020 года и далее"](https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx) представлена на веб-сайте.

# 4 Организационные структуры

4.1 МСЭ провел технические оценки готовности к созданию групп реагирования на компьютерные инциденты (CIRT) в более чем 80 странах и принимает необходимые последующие меры для оказания помощи Государствам-Членам в их осуществлении. В 2020 году МСЭ провел оценки CIRT в Гайане и на Бермудских Островах, а также завершил подготовку отчета об оценке в Либерии. Была успешно завершена работа, связанная с непосредственным участием в создании и/или укреплении 14 национальных CIRT, и из 7 текущих проектов 3 находятся в процессе завершения, которое запланировано на первый квартал 2021 года. МСЭ и правительство Багамских Островов также подписали соглашение о сотрудничестве, в частности, для формирования национальной CIRT.

4.2 По состоянию на настоящее время МСЭ организовал 29 [учений по кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), в которых приняли участие более 100 стран. В сентябре-декабре 2020 года МСЭ была организована и осуществлена программа ["Глобальные учения МСЭ по кибербезопасности 2020 года"](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx), в рамках которой был проведен ряд онлайновых мероприятий, включающих региональные диалоги, вебинары по техническим и стратегическим вопросам, курсы подготовки по использованию инструментов и формирования навыков, а также региональную программу ["Учения по кибербезопасности 2020 года" для тихоокеанских островов](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2020/Pacific%20Cyberdrill/Pacific-Cyberdrill21.aspx).

# 5 Создание потенциала

5.1 В рамках [Глобальных учений МСЭ по кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) БРЭ организовало региональные форумы по кибербезопасности для всех регионов МСЭ в целях укрепления кадрового и организационного потенциала.

5.2 После ВКРЭ-17 Группа Докладчика по Вопросу 3/2 ([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)) продолжает свою работу в исследовательский период 2018−2021 годов.

5.3 Процесс обновления [Руководства по разработке национальной стратегии кибербезопасности (NCS)](https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018) продолжается и, как ожидается, будет завершен в октябре 2021 года. В настоящее время в работе по обновлению принимают участие более 20 структур. Также 19 октября 2020 года МСЭ организовал вебинар: "[Национальные стратегии кибербезопасности: реализация и мониторинг](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/2020-NCS-IM-webinar.aspx)", в рамках которого обсуждался вопрос жизненного цикла разработки и реализации NCS. Были инициированы мероприятия по оказанию технической помощи в области NCS для Фиджи, Либерии и Чада, и в настоящее время ведутся обсуждения с другими Государствами-Членами, нуждающимися в помощи. 20 февраля 2020 года в Мельбурне, Австралия, был проведен региональный семинар для Азиатско-Тихоокеанского региона на тему "[Жизненный цикл и разработка национальных стратегий кибербезопасности](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/ITU-regional-workshop-national-cybersecurity-strategies.aspx)". Также на завершающем этапе находится работа МСЭ над онлайновыми учебными материалами по развитию NCS, которые будут представляться в рамках Академии МСЭ во втором квартале 2021 года.

5.4 В рамках деятельности [Академии МСЭ](https://academy.itu.int/training-courses/full-catalogue?search_api_fulltext=&field_taxon_registration=All&field_course_fee=All&field_taxon_region=All&field_taxon_type=All&field_taxon_topics=109&field_taxon_languages=All&date_start=&date_end=&items_per_page=10) Союз и ЦПМ продолжают проводить подготовительные мероприятия и семинары-практикумы, посвященные различным областям сферы кибербезопасности.

5.5 Для решения задач, связанных с кибербезопасностью, в условиях пандемии COVID-19 и для [обеспечения инфраструктуры здравоохранения Государств-Членов своевременной информацией о киберугрозах](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Covid-19-CNI-Solution.aspx) Член Сектора МСЭ компания BitSight предоставила Государствам-Членам МСЭ доступ к своей платформе балльной оценки кибербезопасности.

5.6 Была начата и в настоящее время ведется работа над четвертой итерацией обследования для [Глобального индекса кибербезопасности МСЭ (GCI)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx), включающей усовершенствованные методы и вопросник. Обследование GCI было завершено 30 сентября 2020 года. Помимо экспертов из академических организаций и частного сектора всем Государствам-Членам было предложено назначить экспертов для представления вкладов и участия в [собрании Группы экспертов по определению весовых коэффициентов для GCI](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx), которое состоялось 15 октября 2020 года.

5.7 В целях содействия привлечению молодежи к деятельности в области кибербезопасности и решения общемировой проблемы нехватки кадров в данной сфере МСЭ приступит к осуществлению инициативы "Youth4Cyber".

5.8 МСЭ также завершает разработку плана начала осуществления программы наставничества "Женщины в киберсфере", направленной на укрепление потенциала женщин-профессионалов младшего уровня, желающих начать работу или преуспеть в области кибербезопасности.

# 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 поручению сессии Совета 2019 года Генеральный секретарь представит следующей сессии Совета: 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. В соответствии с процессом разработки проекта Руководящих указаний, сформулированным Советом 2019 года, и после первых онлайновых открытых консультаций, состоявшихся 23 апреля 2020 года для всех заинтересованных сторон ВВУИО для целей представления замечаний по проекту Руководящих указаний, вторые онлайновые открытые консультации для всех заинтересованных сторон ВВУИО будут проведены 1 марта 2021 года.

6.3 Выполняя функции основной содействующей организации по выполнению Направления деятельности С5 ВВУИО, МСЭ организовал ряд собраний в рамках [Форума ВВУИО 2020 года](https://www.itu.int/net4/wsis/forum/2020/en), в том числе собрание содействующей организации по направлению деятельности С5 по теме "Кибербезопасность в эпоху квантовых информационных технологий (QIT): проблемы и соображения, касающиеся сетей ИКТ", а также диалог высокого уровня на тему "Обеспечение заслуживающего доверия медицинского обслуживания в мире искусственного интеллекта".

# 7 Защита ребенка в онлайновой среде (COP)

7.1 Многосторонняя рабочая группа экспертов, в которой представлены более 50 организаций и отдельных экспертов из различных секторов, рассмотрела четыре набора [Руководящих указаний по защите ребенка в онлайновой среде, предназначенных для директивных органов, представителей отрасли, родителей и педагогов, а также детей](https://www.itu.int/en/cop/Pages/guidelines.aspx). После [глобальной презентации новых Руководящих указаний](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/2020-COP-Guidelines-launch-webinar.aspx) были проведены [региональные мероприятия](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/2020/Regional-Launches-COP-2020-Guidelines.aspx) с целью обсуждения возможностей их реализации на региональном и национальном уровнях.

7.2 В Африке, до представления Руководящих указаний в этом регионе, были организованы первые подготовительные курсы на английском и французском языках для представителей директивных органов, занимающихся вопросами СОР. В регионе СНГ региональное отделение МСЭ для СНГ совместно с Одесской национальной академией связи имени А.С. Попова разработало [курс безопасного пользования ресурсами сети интернет](https://onlinesafety.info/" \l "/home). В Азиатско-Тихоокеанском регионе в рамках совместного проекта с Министерством связи и искусств (DoCA) Австралии на основе Руководящих указаний по СОР в координации с другими партнерами была предоставлена помощь в разработке национальных стратегий СОР и связанных с ними систем для шести малых островных и развивающихся государств. В Северной и Южной Америке начались обсуждения с Колумбией, Коста-Рикой, Бразилией и Парагваем по вопросам разработки и реализации национальных рамочных стратегий. Был достигнут значительный прогресс во внедрении Руководящих указаний по СОР в Европе, где проводились многочисленные мероприятия в рамках региональной инициативы по укреплению доверия и уверенности при использовании ИКТ.

7.3 Королевство Саудовская Аравия и МСЭ подписали соглашение об осуществлении трехлетней глобальной программы "Создание безопасной и расширяющей права и возможности киберсреды для детей", в рамках которой основное внимание уделяется как помощи правительствам в разработке стратегии, так и развитию цифровых навыков и грамотности у конечных пользователей. Начало реализации программы запланировано на 1 квартал 2021 года.

7.4 Был опубликован отчет "[Положение дел в национальных экосистемах защиты ребенка в онлайновой среде в странах Юго-Восточной Европы](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/FINAL%20REPORT.pdf)", после которого состоялись многочисленные мероприятия и форумы, которые были посвящены полностью или частично вопросу защиты ребенка в онлайновой среде в Европе.

7.5 МСЭ отпраздновал День более безопасного интернета 2021 года, опубликовав различные сообщения, включая запись в [блоге](https://www.itu.int/en/myitu/News/2021/02/08/18/38/Sango-Internet-safety-drawing-child-online-protection-COP) об использовании талисмана в области защиты ребенка в онлайновой среде в рамках национального конкурса рисунков в Венгрии. Также было объявлено об использовании талисмана COP в [совместном проекте с Eni и Deloitte Italia](https://www.bing.com/videos/search?q=sango+announcing+eni+youtube&docid=13903411089711&mid=271E2ABE304F85C97D50271E2ABE304F85C97D50&view=detail&FORM=VIRE), направленном на повышение осведомленности и укрепление потенциала в области онлайновой безопасности среди детей и педагогов.

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