|  |  |
| --- | --- |
| **СОВЕТ 2022Женева, 21–31 марта 2022 года** |  |
|  |  |
|  |  |
| **Пункт повестки дня: PL 1.4** | **Документ C22/18-R** |
| **18 февраля 2022 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 в 2021 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).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*](https://www.itu.int/md/D14-WTDC17-C-0115/en) *(Пересм. Буэнос-Айрес, 2017 г.) 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), [C20/18](https://www.itu.int/md/S20-CL-C-0018/en) и [C21/18](https://www.itu.int/md/S21-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-я Исследовательская комиссия МСЭ-Т (ИК17)](http://www.itu.int/ITU-T/studygroups/com17/), 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 два собрания в апреле и августе/сентябре 2021 года, на которых ИК17 создала 22 [новых направления работы по стандартизации](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17), а также провела два электронных пленарных заседания в январе 2021 года и январе 2022 года. ИК17 утвердила более 30 новых или пересмотренных Рекомендаций МСЭ-Т по безопасности в области ИКТ, а именно X.1011, X.1046, X.1047, X.1054 (пересмотрена), X.1060, X.1061, X.1080.2, X.1217, X.1233, X.1234, X.1235, X.1252, X.1333, X.1369, X.1376, X.1405, X.1406, X.1407, X.1408, X.1453, X.1470, X.1643, X.1712, X.1752, X.1770, X.1811 и X.Suppl.36.

3.3 ИК17 также согласовала Технический отчет "Структура стандартизации безопасности для виртуализированных услуг".

3.4 ИК3 МСЭ-T продолжает исследование экономических и политических аспектов больших данных и цифровой идентичности, относящихся к услугам международной электросвязи, в рамках Вопроса 11/3. Недавно ИК3 утвердила [Рекомендацию МСЭ-T D.1102 "Механизмы компенсации потребителям и защиты потребителей OTT"](https://www.itu.int/rec/T-REC-D.1102).

3.5 ИК11 МСЭ-T продолжает заниматься проблематикой совершенствования протоколов сигнализации на предмет повышения их защищенности, включая разработку дополнительных требований к обмену сигнальными сообщениями, а также специальных протоколов. ИК11 МСЭ-T согласовала Технический отчет QSTR-USSD "Требующее малого объема ресурсов, квантовоустойчивое шифрование сообщений USSD для использования в финансовых услугах" и Добавление Q.Suppl.75, касающееся борьбы с контрафактными и похищенными устройствами электросвязи/ИКТ.

3.6 ИК9 МСЭ-T утвердила пересмотренные Рекомендации [МСЭ-T J.1026](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14868), [J.1027](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14869), [J.1028](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14870) и [J.1204](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14357). Также ИК9 утвердила J.1205 и продолжила работу над обновлением Руководства пользователя Рекомендацией МСЭ-T [J.1012](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13573) и двумя Добавлениями 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) и [J.Sup8](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14287).

3.7 ИК13 МСЭ-T утвердила следующие Рекомендации: МСЭ-Т Y.3056 и Y.3057 об основанном на доверии управлении личными данными и МСЭ-Т Y.3805 и Y.3806 о сетях квантового распределения ключей.

3.8 ИК15 МСЭ-T согласовала МСЭ-T G.Suppl.OTNsec "Безопасность оптических транспортных сетей".

3.9 ИК16 МСЭ-T утвердила Рекомендацию МСЭ-T F.747.10 "Требования к системам распределенного реестра (DLS) для услуг, использующих защищенный человеческий фактор" (готовится к публикации), в которой описаны общие требования и функциональные возможности систем распределенного реестра (DLS) для услуг, использующих защищенный человеческий фактор.

3.10 ИК20 МСЭ-T были разработаны следующие Рекомендации, касающиеся безопасности: [Y.4808](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14381), Y.4810 и Y.4811.

3.11 Несколько оперативных групп МСЭ-Т в рамках своей работы изучают аспект доверия к различным появляющимся технологиям. К их числу относятся: 1) *[Оперативная группа МСЭ-Т "Федерации испытательных стендов для IMT-2020 и последующих систем" (ОГ-TBFxG)](https://www.itu.int/en/ITU-T/focusgroups/tbfxg/Pages/default.aspx)*, 2) *[Оперативная группа МСЭ-T по искусственному интеллекту (ИИ) и интернету вещей (IoT) для цифрового сельского хозяйства (ОГ‑AI4A)](https://www.itu.int/en/ITU-T/focusgroups/ai4a/Pages/default.aspx)*, 3) *[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)*, 4) *[Оперативная группа МСЭ по автономным сетям (ОГ-AN)](https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx)*, 5) *[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)*,6) *[Оперативная группа МСЭ-T по экологической эффективности для искусственного интеллекта и других возникающих технологий (ОГ-AI4EE)](https://www.itu.int/en/ITU-T/focusgroups/ai4ee/Pages/default.aspx)*, 7) *[Оперативная группа МСЭ-T по искусственному интеллекту для здравоохранения (ОГ-AI4H)](https://www.itu.int/en/ITU-T/focusgroups/ai4h)* и 8) *[Оперативная группа МСЭ-Т по мультимедиа в автотранспортных средствах (ОГ-VM)](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx).*

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). 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 В 2021 году МСЭ провел технические оценки готовности к созданию групп реагирования на компьютерные инциденты (CIRT) более чем в 80 странах и принимает необходимые последующие меры для оказания помощи Государствам-Членам в их осуществлении. К началу 2021 года была успешно завершена работа, связанная с непосредственным участием в создании и/или укреплении 17 национальных CIRT; три (3) проекта были успешно завершены в 2021 году; была проведена оценка CIRT для Гвинеи-Бисау, Багамских Островов, Монголии и Гайаны; был рассмотрен проект CIRT для Эсватини; в настоящее время продолжается реализация четырех проектов внедрения CIRT. МСЭ также оказал помощь Мали и Малави в разработке проектов национальной инфраструктуры открытых ключей (PKI) для каждой из стран.

4.2 На настоящий момент МСЭ организовал 34 [учения по кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), в которых приняли участие более 120 стран. В сентябре–декабре 2021 года МСЭ была организована и проведена программа ["Глобальные учения МСЭ по кибербезопасности 2021 года"](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyberdrills-2021.aspx), в рамках которой состоялся ряд онлайновых мероприятий, включающих региональные диалоги, вебинары по техническим и стратегическим вопросам, курсы подготовки по использованию инструментов и формированию навыков, а также два субрегиональных учения по кибербезопасности для стран ЭКОВАС и САДК и одно национальное учение по кибербезопасности для Индии. Кроме того, в 2021 году были подготовлены две публикации: "Оперативные рамки и руководящие принципы планирования и проведения региональных учений МСЭ по кибербезопасности" и "Программа МСЭ по кибербезопасности: структура CIRT".

# 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)) продолжила свою работу в исследовательском периоде 2018−2021 годов.

5.3 МСЭ содействовал обновлению [Руководства по разработке национальной стратегии кибербезопасности (NCS)](https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018). Более [20 организаций](https://ncsguide.org/partners/) внесли свой вклад в работу над вторым [изданием Руководства](https://ncsguide.org/the-guide/), представленным в ноябре 2021 года в рамках глобального вебинара, на котором рассматривался вопрос жизненного цикла разработки и реализации NCS, обсуждались имеющиеся проблемы и возможности и прозвучал призыв к расширению сотрудничества. Были инициированы мероприятия по оказанию технической помощи в области NCS для Багамских Островов, Руанды, Марокко и региона САДК, и в настоящее время ведутся обсуждения с другими Государствами-Членами, нуждающимися в поддержке. МСЭ также подготовил и сделал доступным на платформе Академии МСЭ учебный курс ["Жизненный цикл, принципы и передовой практический опыт в области разработки и осуществления национальных стратегий кибербезопасности"](https://academy.itu.int/training-courses/full-catalogue/lifecycle-principles-and-good-practices-national-cybersecurity-strategy-development-and) в онлайновой форме на трех языках (английский, французский, испанский). Версия учебного курса на русском языке будет доступна в марте 2021 года. МСЭ сотрудничает с Группой Всемирного банка для организации региональных вебинаров, в рамках которых можно познакомиться с оперативной информацией о том, как разработать план действий в области NCS. МСЭ разрабатывает инструмент установления контрольных показателей NCS для поддержки Государств-Членов и специалистов-практиков в области кибербезопасности в их работе, связанной с NCS. Подготовка пилотной версией инструмента была завершена в январе, а его дальнейшее обновление будет вестись в 2021 году.

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 центры профессионального мастерства (ЦПМ) продолжают проводить подготовительные мероприятия и семинары-практикумы, посвященные различным областям кибербезопасности.

5.5 Презентация четвертого издания отчета по [Глобальному индексу кибербезопасности (GCI) МСЭ](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) состоялась [29 июня 2021 года](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI/GCIv4-Report-Launch.aspx). В этом издании освещены 193 Государства-Члена и Государство Палестина; данные были предоставлены 169 странами. Уже ведется работа по обновлению вопросника для GCI. В октябре 2021 года Группе Докладчика по Вопросу 3 2-й Исследовательской комиссии МСЭ-Т в виртуальном режиме был представлен новый набор документов, и Исследовательская группа создала виртуальную группу, работающую по переписке, для внесения вклада в подготовку пересмотренного вопросника. Ожидается, что новое издание вопросника для GCI будет выпущено в начале 2022 года.

5.6 В целях содействия вовлечению молодежи в деятельность в области кибербезопасности и повышению осведомленности об общемировой проблеме нехватки кадров в данной сфере МСЭ планирует проведение мероприятий и осуществление различных форм сотрудничества для молодежи и с ее участием под эгидой инициативы "Поколение подключений".

5.7 МСЭ также успешно завершил первый цикл программы наставничества "Женщины в сфере кибербезопасности", направленной на укрепление потенциала женщин-профессионалов младшего уровня, желающих начать работу или преуспеть в области кибербезопасности. Новый цикл должен начаться в апреле 2022 года с участием целевых групп в Африке, арабских странах и Азиатско-Тихоокеанском регионе.

# 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 В ходе сессии 2019 года Совет поручил Генеральному секретарю представить Совету для рассмотрения и утверждения руководящие указания по использованию Глобальной программы кибербезопасности (GCA). [Документ C21/71](https://www.itu.int/md/S21-CL-C-0071/en) был соответствующим образом подготовлен и представлен Генеральным секретарем в рамках виртуальных консультаций Советников в 2021 году (C21/VCC-1). После обсуждений на C21/VCC-1 Государства – Члены Совета поручили секретариату "провести дальнейшие консультации с Государствами – Членами Совета, учитывая полученные вклады и сделанные на данном собрании замечания. Секретариату следует вновь представить пересмотренный Документ 71 для рассмотрения и утверждения на следующей сессии Совета". В настоящее время ведутся консультации с Государствами – Членами Совета; пересмотренный документ будет представлен Совету в 2022 году для рассмотрения и утверждения.

6.3 Выполняя функции основной содействующей организации по Направлению деятельности С5 ВВУИО, МСЭ организовал в рамках [Форума ВВУИО 2021 года](https://www.itu.int/net4/wsis/forum/2020/en) специальный сегмент собраний, в том числе собрание содействующей организации по Направлению деятельности С5 по теме "Кибербезопасность: способы обеспечения многомерной кибербезопасности – Возможности и сложные задачи в использовании индексов для понимания кибербезопасности", вторые открытые консультации по проекту руководящих указаний по использованию ГПК, а также диалог высокого уровня на тему "Проверка готовности к ИИ: воздействие на политику, возможности и сложные задачи".

# 7 Защита ребенка в онлайновой среде (COP)

7.1 Защита ребенка в онлайновой среде вошла в совместный проект МСЭ и ЮНИСЕФ Giga в качестве одного из ключевых элементов четвертого направления.

7.2 МСЭ также подписал соглашение о сотрудничестве в этой области с Фондом SCORT. МСЭ участвовал во многих обсуждениях, в частности в рамках Дня более безопасного интернета 2021 года, 15-й Европейской конференции "Футбол в интересах развития" и круглых столов с участием европейских футбольных клубов.

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. Реализация программы началась в 2021 году с подписания внутреннего проектного документа МСЭ. Первым шагом МСЭ в реализации проекта было создание потенциала посредством разработки для всех соответствующих заинтересованных сторон проводимых по гибкому графику курсов онлайновой подготовки и других интерактивных решений, позволяющих детям и молодежи стать ответственными цифровыми гражданами.

7.4 Все регионы МСЭ приступили к проведению мероприятий в рамках Глобального проекта "Создание безопасной онлайновой среды, расширяющей права и возможности детей". Первой страной, реализующей проект, стала Албания, за которой последовали Малави и Марокко.

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. Помимо этого, талисман COP выступал модератором на различных виртуальных мероприятиях, таких как пятиминутка по вопросам безопасности в онлайновой среде в рамках [Дня "Девушки в ИКТ"](https://www.itu.int/women-and-girls/girls-in-ict/girlsinict-online-safety-moment/) и сессия 4 ГСР-21, которая была посвящена теме ["Безопасный охват цифровыми технологиями – Защита ребенка в онлайновой среде"](https://www.itu.int/en/ITU-D/Conferences/GSR/2021/Pages/global.aspx).

7.6 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. В [курсе "Безопасность в онлайновой среде с Санго"](https://www.itu-cop-guidelines.com/children), состоящем из пяти выпусков, детям младше девяти лет даются практические советы в отношении рисков, с которыми они могут столкнуться в онлайновой среде.

7.7 В рамках Академии МСЭ Союз организовал для регуляторных органов Арабского региона учебный курс по защите ребенка в онлайновой среде.

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