|  |  |
| --- | --- |
| **Пункт повестки дня: PL 2** | **Документ C25/18-R** |
| **16 мая 2025 года** |
| **Оригинал: английский** |
|  |  |
| Отчет Генерального секретаря |
| Виды деятельности МСЭ по усилению роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий |
| **Назначение**В настоящем отчете содержится краткое описание видов деятельности МСЭ, которые осуществлялись в 2024–2025 годах в связи с Резолюцией 130 (Пересм. Бухарест, 2022 г.), роли МСЭ как единственной содействующей организации по Направлению деятельности С5 ВВУИО, а также других решений членов МСЭ по усилению роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ).**Необходимые действия Совета**Совету предлагается **принять к сведению** настоящий отчет.**Соответствующая увязка со Стратегическим планом**Содействие универсальной возможности установления соединений; устойчивая цифровая трансформация; инклюзивные и защищенные инфраструктура и услуги электросвязи/ИКТ.**Финансовые последствия**В рамках выделенного бюджета на 2024–2025 годы.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Справочные материалы***Резолюции* [*71*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-071-R.pdf)*,* [*130*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-130-R.pdf)*,* [*140*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-140-R.pdf)*,* [*179*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-179-R.pdf) *(Пересм. Бухарест, 2022 г.), Резолюции*[*174*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-174-R.pdf) *(Пересм. Пусан, 2014 г.),* [*181*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-181-R.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, 2, 67, 69 (Пересм. Кигали, 2022 г.) ВКРЭ*](https://www.itu.int/dms_pub/itu-d/opb/tdc/D-TDC-WTDC-2022-PDF-R.pdf)*; Приоритеты МСЭ-D ([Кигалийский план действий](https://www.itu.int/md/D14-WTDC17-C-0115/en)); Резолюции* [*50*](https://www.itu.int/pub/T-RES-T.50-2022) *(Пересм. Женева, 2022 г.),* [*52*](https://www.itu.int/pub/T-RES-T.52-2022) *(Пересм. Хаммамет, 2016 г.),* [*75*](https://www.itu.int/pub/T-RES-T.75-2022) *(Пересм. Женева, 2022 г.),* [*58*](https://www.itu.int/pub/T-RES-T.58-2022) *(Пересм. Женева, 2022 г.) Всемирной ассамблеи по стандартизации электросвязи; 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)*,* [*C21/18*](https://www.itu.int/md/S21-CL-C-0018/en)*,* [*C22/18*](https://www.itu.int/md/S22-CL-C-0018/en)*,* [*C23/38*](https://www.itu.int/md/S23-CL-C-0038/en)*,* [*C24/18*](https://www.itu.int/md/S24-CL-C-0018/en) *Совета* |

В настоящем документе содержится информация о деятельности МСЭ в связи с Резолюцией 130 (Пересм. Бухарест, 2022 г.) Полномочной конференции (ПК), роли МСЭ в качестве ведущей содействующей организации по Направлению деятельности C5 ВВУИО и других решениях членов по усилению роли МСЭ в укреплении доверия и безопасности при использовании ИКТ.

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.

# 1 Меры правового характера

В рамках приоритета 5 МСЭ-D согласно Кигалийскому плану действий и с учетом Вопроса 3/2 МСЭ-D МСЭ помогает Государствам-Членам понять правовые аспекты кибербезопасности с помощью [ресурсов МСЭ по законодательству в области киберпреступности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx). МСЭ тесно сотрудничает с такими партнерами, как Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН).

# 2 Технические и процедурные меры

2.1 [17-я Исследовательская комиссия МСЭ-Т (ИК17)](http://www.itu.int/ITU-T/studygroups/com17/) провела два собрания – в сентябре 2024 года и в апреле 2025 года, – создала 50 новых направлений работы по стандартизации и утвердила 36 новых или пересмотренных Рекомендаций по безопасности искусственного интеллекта, систем Международной подвижной электросвязи, облачных вычислений, интернета вещей, интеллектуальных транспортных систем, систем цифровых двойников, распределения квантовых ключей, управления доступом, цифровых финансовых услуг, сохранения конфиденциальности и других интеллектуальных услуг. Кроме того, ИК5, 11, 13, 15, 20 и 21 МСЭ-Т утвердили рекомендации по безопасности ИКТ (см. [каталог Рекомендаций МСЭ‑Т](https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx)) по широкому кругу вопросов – от борьбы с контрафактными и похищенными мобильными устройствами ИКТ, степени доверия в отношении IMT-2020 и дальнейших поколений, инфраструктуры (например, электросетей, пассивных оптических сетей), конвергенции фиксированной, подвижной и спутниковой связи, а также безопасности IoT до метавселенной и "умных" городов, управления цифровыми правами для распределения видео-/аудиоконтента и установления аутентичности мультимедиа.

2.2 ИК11 продолжает деятельность по [безопасности сигнализации](https://itu.int/go/SIG-SECURITY) для борьбы с контрафактными и похищенными мобильными устройствами ИКТ и с атаками на телефонные сети (такими как телефонный спам, роботизированные вызовы, поддельные номера и т. д.). После Рекомендаций МСЭ-T Q.3057 (2020 г.), где описано использование цифровых подписей (цифровых сертификатов) при обмене сигнализацией, Q.3062 (2022 г.) "Процедуры и протоколы сигнализации для обеспечения возможности присоединения доверенных сетевых объектов для поддержки существующих и появляющихся сетей" и Q.3063 (2022 г.) "Процедуры сигнализации при аутентификации идентификации линии вызывающего абонента" ИК11 утвердила в 2023 году поправки к стандартам SS7 и BICC для поддержки аутентификации идентификации линии вызывающего абонента, а также Рекомендацию Q.5054 "Ориентированная на потребителей система борьбы с использованием контрафактных и похищенных мобильных устройств ИКТ".

2.3 МСЭ-R разработал четкие принципы безопасности для сетей Международной подвижной электросвязи (IMT) (3G, 4G и 5G). Он также опубликовал Рекомендации по вопросам безопасности в архитектуре сетевого управления для цифровых спутниковых систем и по улучшению качественных показателей протокола управления передачей по спутниковым сетям (см. [здесь](https://www.itu.int/pub/R-REC)). Информация о будущих системах подвижной связи – "IMT на период до 2020 года и далее" – представлена [здесь](https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx).

# 3 Организационные структуры

3.1 Начиная с 2012 года МСЭ сотрудничает с Государствами-Членами, партнерами и глобальными организациями в целях укрепления кибербезопасности путем создания национальных и региональных [групп реагирования на компьютерные инциденты (CIRT)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx). Кроме того, МСЭ проводит оценки зрелости CIRT для дальнейшего расширения их возможностей. На сегодняшний день МСЭ оказал помощь 85 странам в оценке их готовности к обеспечению кибербезопасности, что позволило создать или усовершенствовать национальные CIRT. В настоящее время МСЭ работает над внедрением CIRT в четырех странах.

МСЭ продолжает активно сотрудничать с сообществом FIRST в целях совершенствования структуры обслуживания групп реагирования на инциденты в сфере компьютерной безопасности (CSIRT) и пересмотра учебных материалов для создания потенциала в области управления деятельностью национальных CIRT.

3.2 По состоянию на май 2025 года МСЭ организовал более 55 международных, региональных или национальных [тренировочных занятий по кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) (включая три глобальных тренировочных занятия) с участием более 160 стран во всех шести регионах МСЭ. Вторые глобальные тренировочные занятия по кибербезопасности состоялись в мае 2025 года и были организованы Советом по кибербезопасности Объединенных Арабских Эмиратов.

# 4 Создание потенциала

4.1 БРЭ организовало региональные форумы по кибербезопасности для всех регионов МСЭ в целях создания потенциала.

После ВКРЭ-22 продолжается работа над Вопросом 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)).

4.2 МСЭ совместно с 20 международными партнерами ведет подготовку обновленной версии Руководства по разработке национальной стратегии кибербезопасности (NCS). В основу обновленной версии Руководства, которая, как ожидается, будет опубликована в IV квартале 2025 года, ляжет его [второе издание](https://ncsguide.org/), вышедшее в 2021 году. МСЭ использует данное Руководство в работе с несколькими странами и территориями для совершенствования их стратегий в области кибербезопасности путем проведения очных настольных учений и оценки планов действий, в частности в сотрудничестве с Соединенным Королевством и Японией.

4.3 МСЭ посредством 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), центров профессионального мастерства МСЭ и центров профессиональной подготовки Академии продолжает проводить мероприятия в области профессиональной подготовки и семинары-практикумы, посвященные различным аспектам кибербезопасности. Так, в 2021 году был выпущен [онлайновый курс для самостоятельного изучения](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx), основанный на Руководстве по NCS, который в 2023 году в рамках Академии МСЭ прослушали более 730 участников из 131 страны.

4.4 В ходе пятого обследования для составления [Глобального индекса кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) МСЭ, начатого в сентябре 2024 года, были собраны данные по 172 странам. Ожидается, что сбор данных для следующего GCI начнется в начале 2026 года.

4.5 В 2024 году в рамках усилий по развитию цифровых навыков при поддержке GIZ и Microsoft была успешно реализована программа "[Ее киберследы](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx)" (Her CyberTracks), ориентированная на женщин – сотрудников директивных и дипломатических органов, а также совместно с УНП ООН был обеспечен охват потребностей в области реагирования на инциденты и борьбы с киберпреступностью. По состоянию на 2025 год география программы расширилась, и теперь она ведется не только в пяти странах Северной и Южной Америки (в сотрудничестве с Организацией американских государств (ОАГ)) и странах Европы, которые ранее являлись целевыми, но и во всех странах – членах Африканского союза.

4.6 МСЭ при поддержке Республики Корея работает с 30 странами в рамках программы ["Кибертехнологии во благо"](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyber4Good/Cyber4Good.aspx), предоставляя при посредстве восьми Членов Сектора МСЭ-D бесплатный доступ к инструментам, образовательным материалам и услугам, в том числе к оценкам NCS, инструментам мониторинга киберуязвимости и учебным курсам по цифровым навыкам.

4.7 МСЭ совместно с ОАГ занимался разработкой [системного подхода к образованию в области кибербезопасности](https://www.itu.int/hub/publication/d-phcb-cyb_educ-2024/) и в настоящий момент готовит руководство для стран по его внедрению.

# 5 Международное сотрудничество

5.1 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 ОАГ, ENISA, Интерполом, ЭКОВАС, Всемирным банком, FIRST, GFCE и региональными ассоциациями CSIRT/CERT, такими как AP CERT, AFRICA CERT и OIC CERT, с целью избежать ненужного дублирования работы и определить области для сотрудничества.

5.2 Во исполнение [Решения 630 (2023 г.) Совета](https://www.itu.int/md/S23-CL-C-0124/en) МСЭ разработал [информационный ресурс](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Council/CD630/Global-Cybersecurity-Knowledgebase.aspx) на основе ответов Государств-Членов для оказания им помощи в создании потенциала в области кибербезопасности и киберустойчивости. Свой вклад в создание этого ресурса внесли девять (9) Государств-Членов.

5.3 В качестве ведущей содействующей организации по Направлению деятельности C5 ВВУИО МСЭ организовал сессию содействующих организаций по Направлению деятельности C5 на тему ["Под водой: обеспечение глобальной возможности установления соединений с помощью защищенных подводных сетей"](https://www.itu.int/net4/wsis/forum/2024/Agenda/Session/170) во время [Форума ВВУИО 2024 года](https://www.itu.int/net4/wsis/forum/2024/en), в ходе которого также прошло несколько сессий, посвященных вопросам доверия и уверенности в областях, связанных с новыми и появляющимися технологиями, такими как, например, ИИ и квантовые технологии, а также защита женщин и детей в онлайновой среде. МСЭ планирует провести сессию по Направлению деятельности C5 на [Форуме ВВУИО 2025 года](https://www.itu.int/net4/wsis/forum/2025/).

5.4 МСЭ продолжает взаимодействие с [заинтересованными сторонами в рамках Рабочей группы открытого состава (РГОС) по вопросам безопасности и использования ИКТ](https://meetings.unoda.org/meeting/57871), занимаясь анализом развития потенциала, выявлением текущих потребностей в кибербезопасности на основе Глобального индекса кибербезопасности и демонстрацией результатов инициативы "Ее киберследы".

5.5 В ноябре 2024 года МСЭ в партнерстве с Международным комитетом по охране кабелей (МКОК) также создал [Международный консультативный орган по устойчивости подводных кабелей](https://www.itu.int/digital-resilience/submarine-cables/advisory-body/), в состав которого входят 40 руководителей и экспертов из государственного и частного секторов, с целью содействия диалогу и сотрудничеству в области возможных путей и средств повышения устойчивости этого крайне важного типа инфраструктуры, обеспечивающего связь по всему миру и делающего цифровую экономику возможной. Первое очное собрание комитета состоялось во время [Международного саммита по устойчивости подводных кабелей 2025 года (Абуджа, Нигерия, 26–27 февраля 2025 г.)](https://www.itu.int/digital-resilience/submarine-cables/events/about-nigeria-summit/), на котором представители правительств, ведущих компаний отрасли и международных организаций собрались для решения важнейших проблем в области работы подводных кабелей.

# 6 Защита ребенка в онлайновой среде (COP)

6.1 По состоянию на апрель 2025 года МСЭ оказал поддержку в разработке национальных базовых принципов COP или связанных с ними оценок 13 странам: Албании, Армении, Багамским Островам, Бутану, Боливии, Эквадору, Казахстану, Малави, Монголии, Пакистану, Перу, Суринаму и Таиланду. Продолжается оказание поддержки в области политики Андорре, Эсватини и Ливану. Эти базовые принципы носят нормативно-правовой характер и согласуются с международными стандартами и национальными приоритетами в области защиты ребенка.

6.2 Центральное место в работе МСЭ в области COP занимают практические инструменты и цифровые образовательные ресурсы. В 2024–2025 годах в целях поддержки национальной интеграции принципов защиты ребенка 26 стран перевели Руководящие указания МСЭ по СОР на местные языки, в том числе недавно – на кечуа (Эквадор), аймара (Боливия), голландский (Суринам) и мальтийский языки.

6.3 Разработано десять онлайновых курсов для самостоятельного изучения, которые доступны через платформу Академии МСЭ, в том числе в 2024 году благодаря партнерству с ЮНИСЕФ появился специализированный курс для работников отрасли ИКТ. Одновременно в День безопасного интернета в 2025 году были выпущены онлайновые курсы для детей трех возрастных групп, разработанные при участии детей и доступные на всех шести официальных языках ООН.

6.4 В 2025 году в целях поддержки национальных кампаний по повышению осведомленности были разработаны и распространены (например, в Марокко) дополнительные материалы по повышению осведомленности, в том числе брошюры и обучающие видеоролики. В феврале 2024 года МСЭ также участвовал в кампании по распространению Руководящих указаний по СОР в Сербии. В ходе кампании были проведены мероприятия по распространению информации и презентация недавно переведенных на национальный язык материалов. Кампания прошла плодотворно и охватила 957 детей, а также 60 учителей, педагогов и психологов.

6.5 В общей сложности около 170 000 детей приняли участие в образовательных мероприятиях и мероприятиях по расширению прав и возможностей, посвященных вопросам безопасности в онлайновой среде, а 2500 родителей и педагогов и 1000 заинтересованных лиц из государственных органов прошли обучение в рамках семинаров-практикумов, сессий подготовки инструкторов (ToT) и программ электронного обучения. Эти меры по созданию потенциала были реализованы во всех регионах МСЭ, а программы ToT были проведены в таких странах, как Багамские Острова, Коста-Рика, Эквадор, Кыргызстан, Мальдивские Острова, Малави, Мальта, Микронезия, Марокко и Суринам. Дополнительные усилия на страновом уровне еще более расширили охват деятельности по созданию потенциала в области COP. В Эквадоре в сотрудничестве с фондом Scort был проведен учебный вебинар для молодых спортивных тренеров с целью повышения осведомленности о COP в контексте спорта. Кроме того, в Эквадоре были проведены учебные занятия для директивных органов, компаний отрасли ИКТ и представителей гражданского общества.

6.6 Инициатива "Защита через онлайновое участие" (PoP), возглавляемая совместно МСЭ и Специальным представителем Генерального секретаря ООН по вопросу о насилии в отношении детей, объединяет более 30 партнеров – учреждения системы ООН, технологические платформы, организации гражданского общества и академические организации. В рамках этой инициативы ведется разработка руководящих указаний для директивных органов, служб помощи детям и технологических платформ, а их публикация запланирована на 2025 год. Одновременно МСЭ завершает работу над межведомственным совместным заявлением по искусственному интеллекту и защите ребенка в онлайновой среде в рамках сотрудничества с Комитетом по правам ребенка, ЮНИСЕФ и более чем десятью учреждениями-подписантами; заявление, как ожидается, будет принято Комитетом в 2025 году.

6.7 Что касается исследований и инноваций, то результаты, полученные в рамках инициативы PoP, включая взаимодействие с телефонными службами помощи детям, цифровыми платформами и поставщиками услуг, а также с детьми и молодежью, выявили двойственную природу цифровых сред – это пространство, в котором находятся источники возможного вреда, и это критически важные каналы доступа к службам поддержки. Эти выводы определяют переход к использованию подхода, ориентированного на расширение прав и возможностей и превентивные меры для защиты ребенка в онлайновой среде. Помимо этого, в конце 2024 года МСЭ совместно со Всемирной организацией здравоохранения (ВОЗ) начал глобальную совместную исследовательскую работу по созданию Глобальной сети образования и ресурсов по предотвращению инцидентов в сфере безопасности в онлайновой среде. Признавая важность участия детей, в течение 2024 и 2025 годов МСЭ содействовал созданию детских целевых групп в Индонезии, Малави и Ливане, что позволило детям внести непосредственный вклад в разработку национальных стратегий COP.

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