|  |  |
| --- | --- |
| **Пункт повестки дня: PL 2** | **Документ C24/18-R** |
| **18 апреля 2024 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 2023–2024 годах в связи с Резолюцией 130 (Пересм. Бухарест, 2022 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 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.) Полномочной конференции; Резолюции* [*174*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-174-R.pdf) *(Пересм. Дубай, 2018 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.)*](https://www.itu.int/dms_pub/itu-d/opb/tdc/D-TDC-WTDC-2022-PDF-R.pdf) *ВКРЭ; Приоритеты МСЭ-D (*[*Кигалийский план действий*](https://www.itu.int/dms_pub/itu-d/opb/tdc/D-TDC-WTDC-2022-PDF-R.pdf)*); Резолюции* [*50 (Пересм. Женева, 2022 г.)*](https://www.itu.int/pub/T-RES-T.50-2022)*,* [*52 (Пересм. Хаммамет, 2016 г.)*](https://www.itu.int/pub/T-RES-T.52-2022)*,* [*75 (Пересм. Женева, 2022 г.)*](https://www.itu.int/pub/T-RES-T.75-2022)*,* [*58 (Пересм. Женева, 2022 г.)*](https://www.itu.int/pub/T-RES-T.58-2022) *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) *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 единственной 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 Кигалийского плана действий и с учетом Вопроса 3/2 МСЭ-D МСЭ помогает Государствам-Членам разобраться в правовых аспектах 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)](https://www.itu.int/ru/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) провела два собрания в августе–сентябре 2023 года и феврале–марте 2024 года, создала 82 [новых направления работы по стандартизации и утвердила 25 новых или пересмотренных Рекомендаций по вопросам безопасности 5G, облачных технологий, IoT, ИТС, сетей цифровых двойников, квантового распределения ключей, аутентификации, цифровых финансовых услуг и других интеллектуальных услуг](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). Кроме того, ИК 5, 11, 13, 16 и 20 МСЭ-Т утвердили Рекомендации по безопасности ИКТ (см. [каталог Рекомендаций МСЭ-Т](https://www.itu.int/ru/ITU-T/publications/Pages/recs.aspx)) по широкому кругу вопросов – от циркуляционной экономики, электромагнитной безопасности, процедур и протоколов сигнализации, облачных вычислений, сети квантового распределения ключей, доверия к ИКТ, JPEG 2000 до решений oneM2M по обеспечению безопасности.

2.2 Несколько оперативных групп МСЭ-Т, которые упоминаются на [этой странице](https://www.itu.int/en/ITU-T/focusgroups/Pages/default.aspx), изучают в рамках своей работы аспект доверия к различным появляющимся технологиям. Например, Оперативная группа по метавселенной (ОГ-MV) утвердила четыре технических отчета по таким вопросам, как киберриски, угрозы и вред в метавселенной, а также внедрение стандартов безопасности и контроля пользователей над информацией, позволяющей установить личность (PII), при разработке метавселенной.

2.3 ИК13 МСЭ-Т утвердила новые Рекомендации МСЭ-Т Y.3060 "Автономные сети – Обзор аспектов доверия" и Y.TiAN-eval "Оценка степени доверия в отношении IMT-2020 и дальнейших поколений с функциями автономных сетей" на основе итоговых документов ОГ-AN МСЭ-T.

2.4 ИК11 продолжает деятельность по [безопасности сигнализации](https://itu.int/go/SIG-SECURITY) для борьбы с атаками на телефонные сети (такими как телефонный спам, роботизированные вызовы, поддельные номера и т. д.). После 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.

2.5 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/ru)). 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). Кроме того, МСЭ проводит оценки зрелости CIRT для дальнейшего расширения их возможностей. На сегодняшний день МСЭ оказал помощь 84 странам в оценке их готовности к обеспечению кибербезопасности, что привело к созданию или совершенствованию национальных CIRT. В настоящее время МСЭ работает над внедрением CIRT в трех странах.

МСЭ продолжает активно сотрудничать с сообществом FIRST в целях совершенствования структуры обслуживания Группы 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 2024 года МСЭ организовал более 42 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 140 стран и 2500 специалистов во всех шести регионах МСЭ. Первые в истории глобальные очные тренировочные занятия по кибербезопасности запланированы на апрель 2024 года и будут 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](https://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=6&sp=2014&rgq=D14-SG02-RGQ03.2&stg=2)).

4.2 МСЭ в сотрудничестве более чем с 20 международными партнерами участвует в подготовке [второго издания Руководства по разработке национальной стратегии кибербезопасности (NCS)](https://ncsguide.org/), опубликованного в 2021 году, а также в сотрудничестве с Соединенным Королевством работает с несколькими странами и территориями над развитием их стратегий кибербезопасности, проводя очные настольные учения и оценку планов действий. Работу над обновлением Руководства по разработке национальной стратегии кибербезопасности МСЭ совместно с заинтересованными сторонами планирует начать в 2025 году.

4.3 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, МСЭ продолжает проводить мероприятия в области профессиональной подготовки и семинары-практикумы, посвященные различным областям кибербезопасности. В 2021 году был выпущен [онлайновый курс для самостоятельного обучения](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 172 странах были собраны данные в рамках пятого обследования для составления [Глобального индекса кибербезопасности](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) МСЭ. Группа экспертов GCI рекомендовала весовые коэффициенты и способы перехода к модели на основе многоуровневой системы, как это предусмотрено в Резолюции 130 (Пересм. Бухарест, 2022 г.) ПК и Резолюции 46 (Пересм. Кигали, 2022 г.) ВКРЭ.

4.5 В рамках работы по развитию цифровых навыков МСЭ трижды успешно провел программу наставничества МСЭ ["Женщины в сфере кибербезопасности"](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/Women-in-Cyber-Mentorship-Programme.aspx). В третий раз программа началась в апреле 2023 года для целевых групп в Африке, арабском и Азиатско-Тихоокеанском регионах. В 2023 году при поддержке GIZ и Microsoft была успешно проведена программа ["Ее киберследы" (HerCyberTracks)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx), ориентированная на женщин – сотрудников директивных и дипломатических органов; в сотрудничестве с УНП ООН осуществляется развитие программы для охвата конкретных потребностей в области реагирования на инциденты и борьбы с киберпреступностью.

4.6 МСЭ при поддержке Республики Корея работает с 23 странами в рамках программы ["Кибертехнологии во благо"](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyber4Good/Cyber4Good.aspx), предоставляя при посредстве пяти 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 Организацией американских государств занимался разработкой системного подхода к образованию в области кибербезопасности, работает над организацией страновых семинаров-практикумов и помогает странам предпринимать дальнейшие шаги с использованием указанного подхода.

4.8 МСЭ сотрудничал с Королевством Швеция, Microsoft и Глобальным форумом по киберкомпетентности (GFCE) в подготовке Сборника по учету кибербезопасности в процессе развития.

# 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 В соответствии с [Решением 630 (С23)](https://www.itu.int/md/S23-CL-C-0124/en) МСЭ разрабатывает [информационный ресурс](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Council/CD630/Global-Cybersecurity-Knowledgebase.aspx), который поможет Государствам-Членам создавать собственный потенциал кибербезопасности и киберустойчивости, и предложил Государствам-Членам и другим заинтересованным сторонам поделиться для этой цели передовым опытом, ресурсами и соответствующей информацией.

5.3 В качестве ведущей содействующей организации по Направлению деятельности C5 ВВУИО МСЭ организовал сессию содействующих организаций по Направлению деятельности C5 на тему "Устойчивость цифровых технологий: следующая граница – кибер- и космическое пространство" на [Форуме ВВУИО 2023 года](https://www.itu.int/net4/wsis/forum/2023/ru), в ходе которого также прошло несколько сессий, посвященных вопросам доверия и уверенности в областях, связанных с новыми и появляющимися технологиями, такими как, в частности, ИИ, квантовые технологии и так далее, а также защита женщин и детей в онлайновой среде.

5.4 МСЭ продолжает взаимодействие с заинтересованными сторонами в рамках Рабочей группы открытого состава (РГОС) по вопросам безопасности и использования ИКТ, занимаясь анализом развития потенциала, выявлением текущих потребностей в кибербезопасности на основе Глобального индекса кибербезопасности и демонстрацией результатов инициативы HerCyberTracks.

5.5 МСЭ продолжает участвовать в качестве наблюдателя в работе [Специального комитета для разработки всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях](https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home). Функции секретариата специального комитета выполняет УНП ООН.

5.6 В своей работе МСЭ сотрудничает с Государствами-Членами, в частности с Чешской Республикой, Германией, Королевством Саудовская Аравия и Соединенным Королевством.

# 6 Защита ребенка в онлайновой среде (COP)

6.1 В соответствии с соглашением о сотрудничестве между МСЭ и Фондом SCORT, МСЭ выступил одним из организаторов мероприятия на Форуме ВВУИО 2023 года на тему ["Безопасная игра в цифровую эпоху: безопасность детей в онлайновой среде и спорт"](https://www.itu.int/net4/wsis/forum/2023/ru/Agenda/Session/463), которое посвящено использованию потенциала спорта для повышения осведомленности о вопросах безопасности детей в онлайновой среде.

6.2 В соответствии с соглашением, подписанным с Королевством Саудовская Аравия, МСЭ реализует проект "Создание безопасной онлайновой среды, расширяющей права и возможности детей". Проект включает организацию и проведение ряда онлайновых занятий для самостоятельного обучения для всех соответствующих заинтересованных сторон в Академии МСЭ. В середине 2023 года МСЭ планирует представить два интерактивных решения, призванных помочь детям и молодежи стать ответственными цифровыми гражданами, – интернет-приложение и онлайновую игру.

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