|  |  |
| --- | --- |
| **СОВЕТ 2017 Женева, 15–25 мая 2017 года** | logo_R_ |
|  |  |
|  |  |
| **Пункт повестки дня: PL 1.5** | **Документ C17/18-R** |
| **14 марта 2017 года** |
| **Оригинал: английский** |
| Отчет Генерального секретаря | |
| ВИДЫ ДЕЯТЕЛЬНОСТИ МСЭ ПО УСИЛЕНИЮ ЕГО РОЛИ  В УКРЕПЛЕНИИ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ  ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ | |

|  |
| --- |
| Резюме  В настоящем отчете представлено краткое описание видов деятельности МСЭ, которая осуществлялась после сессии Совета 2016 года в связи с Резолюцией 130 (Пересм. Пусан, 2014 г.), роли МСЭ как единственной содействующей организации по Направлению деятельности С5 ВВУИО, а также других решений Членов МСЭ по усилению его роли в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ).  Необходимые действия  Совету предлагается **принять к сведению** настоящий отчет.  \_\_\_\_\_\_\_\_\_\_\_\_  Справочные материалы  [*Резолюция 71 (Пересм. Пусан, 2014 г.)*](http://www.itu.int/en/council/planning/Documents/PP-14_Res71.pdf),[*Резолюция 130 (Пересм. Пусан, 2014 г.)*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20130.pdf),[*Резолюция 140 (Пересм. Пусан, 2014 г.)*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20140.pdf),[*Резолюция 174 (Пересм. Пусан, 2014 г.)*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20174.pdf), [*Резолюция 179 (Пересм. Пусан, 2014 г.)*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20179.pdf),[*Резолюция 181 (Гвадалахара, 2010 г.)*](http://www.itu.int/council/Basic-Texts/ResDecRec-PP10-e.docx#res181),[*Регламент международной электросвязи*](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 [*2*](https://www.itu.int/en/ITU-D/TIES_Protected/WTDC14/WTDC14-FinalReport-E.pdf) *,*[*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf)*,* [*67*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/67revDubai.pdf)*,* [*69*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/69revDubai.pdf) (Пересм. Дубай, 2014 г.) *ВКРЭ, ВКРЭ-14/*[*Задача 3*](https://www.itu.int/en/ITU-D/TIES_Protected/WTDC14/WTDC14-FinalReport-E.pdf) *ДПД*, 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.), Документы* [*C05/32*](http://www.itu.int/md/S05-CL-C-0032/en)*,* [*C05/INF/10*](https://www.itu.int/md/S05-CL-INF-0010/en)*,* [*C06/4*](http://www.itu.int/md/S06-CL-C-0004/en)*,* [*C07/21*](http://www.itu.int/md/S07-CL-C-0021/en)*,* [*C08/33*](http://www.itu.int/md/S08-CL-C-0033/en)*,* [*C09/50*](http://www.itu.int/md/S09-CL-C-0050/en), [*C10/12*](http://www.itu.int/md/S10-CL-C-0012/en)*,* [*C11/54*](http://www.itu.int/md/S11-CL-C-0054/en)*,* [*C12/29*](http://www.itu.int/md/S12-CL-C-0029/en)*,* [*C13/23*](http://www.itu.int/md/S13-CL-C-0023/en), [*C14/23*](http://www.itu.int/md/S14-CL-C-0023/en), [*C15/18*](http://www.itu.int/md/S15-CL-C-0018/en) *и* [*C16/18*](https://www.itu.int/md/S16-CL-C-0018/en) *Совета* |

# 1 Виды деятельности в области кибербезопасности и противодействия спаму

1.1 Развитие ИКТ, основанное на безопасности и доверии, признано важнейшим фактором устойчивого развития. Настоящий отчет, построенный на базе пяти основных составляющих [Глобальной программы кибербезопасности (ГПК)](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx), 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 3 Дубайского плана действий (ДПД) и с учетом Вопроса 3/2 МСЭ‑D (ранее Вопрос 22/1) МСЭ оказывает помощь Государствам-Членам в осмыслении ими правовых аспектов кибербезопасности с использованием [ресурсов МСЭ по законодательству в области киберпреступности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx), чтобы помочь им согласовать свои нормативно-правовые базы.

2.2 В области правовых мер МСЭ тесно сотрудничает с такими партнерами, как УНП ООН и другие организации, обладающие специальными знаниями и опытом в этой сфере.

# 3 Технические и процедурные меры

3.1 [17-я Исследовательская комиссия (ИК17)](http://www.itu.int/ITU-T/studygroups/com17/) МСЭ-Т, ведущая исследовательская комиссия в области безопасности и управления определением идентичности (IdM), продолжает играть важную роль в проведении исследований и разработке стандартов в областях кибербезопасности, борьбы со спамом, IdM, сертификатов X.509 МСЭ-Т, управления информационной безопасностью, повсеместных сенсорных сетей, телебиометрии, безопасности IPTV, безопасности виртуализации с точки зрения безопасности облачных вычислений, а также архитектуры безопасности и безопасности приложений, зачастую в сотрудничестве с внешними организациями и консорциумами по разработке стандартов.

3.2 После Совета МСЭ 2016 года ИК17 утвердила новые Рекомендации МСЭ-Т в области кибербезопасности: Рекомендацию МСЭ‑T X.1038 "Требования безопасности и эталонная архитектура для организации сетей с программируемыми параметрами", Рекомендацию МСЭ‑T X.1039 "Технические меры безопасности для внедрения аспектов безопасности МСЭ-T X.805", Рекомендацию МСЭ‑T X.1085 "Информационные технологии – Методы обеспечения безопасности – Структура телебиометрической аутентификации с использованием модуля защиты биометрического оборудования", Рекомендацию МСЭ‑T X.1087 "Технические и эксплуатационные меры противодействия для телебиометрических приложений, использующих мобильные устройства", Рекомендацию МСЭ‑T X.1258 "Улучшенная аутентификация объектов на основании объединенных атрибутов", Рекомендацию МСЭ‑T X.1542 "Формат обмена информационными сообщениями сеанса", Рекомендацию МСЭ‑T X.1641 "Руководящие указания по безопасности данных клиентов облачных услуг", а также важные пересмотры Рекомендаций серии Х.500 "Информационные технологии – Взаимосвязь открытых систем – Справочник".

3.3 В марте 2017 года планируется утвердить с использованием ТПУ проекты семи Рекомендаций по кибербезопасности, защите информации, позволяющей установить личность, управлению доступом, шифрованию для IoT, восприятию конечным пользователем показателей благонадежности и по возможности безопасного обновления программного обеспечения для интеллектуальных транспортных систем. Планируется завершить для начала процесса утверждения с использованием АПУ проекты еще восьми Рекомендаций по методам обмена структурированной информацией о кибербезопасности, противодействию бот-сетям, использующим смартфоны, противодействию спаму при мгновенной передаче сообщений (SPIM), фишингу через SMS, мерам противодействия кражам мобильных телефонов, а также по безопасности для открытых возможностей служб электросвязи. Начата работа по проектам Рекомендаций по противодействию мошенничеству при предоставлении услуг телефонной связи, безопасности "умных" измерительных услуг в "умных" электросетях, процессу удаления идентифицирующих элементов, гибридной аутентификации и основным механизмам управления в модели клиент-сервер, анализу больших данных при услугах мобильного интернета, безопасности больших данных как услуги, связи как услуги и сети как услуги, телебиометрической аутентификации с использованием био-сигналов, телебиометрическому обнаружению мер, направленных против спуфинга, а также по профилю синтаксиса криптографических сообщений (CMS).

3.4 [Региональная группа ИК17 для Африки](http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/sg17rgafr/Pages/default.aspx) провела свое второе собрание 27−28 июля 2016 года в Хартуме, Республика Судан.

3.5 ИК17 продолжила координацию деятельности с новой ИК20 МСЭ-Т "Интернет вещей и его приложения, включая "умные" города и сообщества (SC&C)" по вопросам безопасности IoT.

3.6 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). Он также выпустил Рекомендации по вопросам безопасности в архитектуре сетевого управления для цифровых спутниковых систем (Рекомендация МСЭ-R S.1250) и по улучшению качественных показателей протокола управления передачей по спутниковым сетям (Рекомендация МСЭ-R S.1711).

# 4 Организационные структуры

4.1 МСЭ продолжает оказывать содействие в создании потенциала на региональном и международном уровнях. МСЭ провел технические оценки для определения степени готовности к [созданию групп реагирования на компьютерные инциденты (CIRT](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx)) в 68 странах и продолжает выполнять необходимые последующие действия. В настоящее время национальные CIRT создаются и совершенствуются в Бурунди, Гамбии, на Кипре и в Кении после успешного завершения соответствующей деятельности в 12 странах.

4.2 МСЭ сотрудничал с Всемирным центром развития потенциала в области кибербезопасности в Oxford Martin School и совместно проводил обзоры потенциала в области кибербезопасности в Таиланде, Сьерра-Леоне и на Мадагаскаре.

4.3 МСЭ продолжает проводить [тренировочные занятия по кибербезопасности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx) для своих стран-партнеров в целях совершенствования возможностей участвующих групп обмениваться информацией и реагировать на инциденты, а также укрепления национального и международного сотрудничества в борьбе с киберугрозами. К настоящему времени МСЭ провел 16 тренировочных занятий по кибербезопасности, в которых приняли участие более 100 стран. В текущем отчетном периоде международные тренировочные занятия по кибербезопасности проведены в Кито, Эквадор, для [региона Северной и Южной Америки](http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2016/15551.aspx) (27 июня–1 июля 2016 г.), в Тунисе, Тунис, для [Арабского региона](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Tunisia_cyberdrill_2016.aspx) (23−27 мая 2016 г.) и на Маврикии для [Африканского региона](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Mauritius_cyberdrill_2016.aspx) (4−8 апреля 2016 г.).

4.4 В настоящее время в рамках усилий многих заинтересованных сторон при содействии МСЭ разрабатывается [комплект материалов по национальной стратегии в области кибербезопасности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx). Для продвижения этой работы состоялись три партнерских [семинара-практикум](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx)а: 18–19 февраля 2016 года в штаб-квартире МСЭ в Женеве, Швейцария, 6−7 июня 2016 года в Saïd Business School, Оксфордский университет, Соединенное Королевство, и 13−14 октября 2016 года в Вашингтоне, О.К., Соединенные Штаты Америки, по приглашению Организации американских государств (ОАГ). Этот продукт находится в процессе завершения и будет представлен широкой общественности до конца 2017 года.

4.5 МСЭ помогал Непалу в разработке национальной политики в области кибербезопасности и в области защиты ребенка в онлайновой среде (4−8 июля 2016 г.), содействовал в повышении уровня информированности и в создании потенциала для примерно 100 правительств, регуляторных органов и заинтересованных сторон из частного сектора, а также продемонстрировал моделирование успешного обеспечения кибербезопасности и активизировал сотрудничество с Управлением электросвязи Непала (NTA).

4.6 Проведены исследования готовности к обеспечению кибербезопасности ряда стран Азиатско-Тихоокеанского региона (2015−2016 гг.) на базе пяти основных составляющих ГПК.

# 5 Создание потенциала

5.1 МСЭ продолжает проводить [региональные форумы по кибербезопасности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) для всех регионов МСЭ, используя их в качестве средства создания потенциала для различных программ и видов деятельности МСЭ-D, а также как рабочую платформу для сотрудничества на региональном и международном уровнях.

5.2В исследовательском периоде 2014–2018 годов 2-я Исследовательская комиссия МСЭ-D продолжает свою работу 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).

5.3 Семинар-практикум ["Стратегия кибербезопасности в странах Африки"](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Pages/default.aspx) был организован совместно МСЭ и АСЭ при поддержке БСЭ и БРЭ 24–26 июля 2016 года в штаб-квартире Национальной корпорации электросвязи (NTC) в Хартуме, Республика Судан.

5.4 Впервые МСЭ установил официальные партнерские отношения с Европейским агентством по безопасности сетей и информации (ENISA) для организации совместного [Регионального форума МСЭ по кибербезопасности](http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/RCYBF/Regional-Cybersecurity-Forum.aspx) 29−30 ноября 2016 года в Софии, Болгария.

5.5 Четвертое собрание ["Платформа для диалога между государственным и частным секторами по вопросам кибербезопасности в странах Центральной Европы"](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/CYBR/Cyber-Security-in-Romania.aspx) было проведено с 14 по 16 сентября 2016 года в Сибу, Румыния.

5.6 В 2014 году были объявлены первые результаты расчета [глобального индекса кибербезопасности](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx) (GCI), а в настоящее время в расширенном кругу партнеров готовится к выпуску [обновленный GCI](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2016.aspx), который был усовершенствован. На настоящее время ответы на вопросник прислали 136 стран, и проводится их анализ.

5.7 В Мьянме, Вьетнаме, Лаосской Народно-Демократической Республике и Камбодже в 2016 году МСЭ помогал в развитии технических навыков для содействия сотрудникам служб реагирования на инциденты.

# 6 Международное сотрудничество

6.1 МСЭ продолжает развивать отношения и [партнерские связи](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) с различными региональными и 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 Выполняя роль ведущей содействующей организации по Направлению деятельности C5 ВВУИО, МСЭ организовал во время [Форума ВВУИО 2016 года](https://www.itu.int/net4/wsis/forum/2016/) несколько мероприятий, способствовавших обмену опытом между всеми группами заинтересованных сторон в рамках глобальных усилий, направленных на содействие укреплению доверия и безопасности при использовании ИКТ.

6.3 Во время Форума Telecom-2016 МСЭ в сотрудничестве с Институтом "Восток − Запад" (EWI), организовал групповую сессию ["ИКТ: доверие, инновации и торговля".](http://www.itu.int/net4/Telecom/webs/TelecomWorld/session/description/C-00001734)

6.4 МСЭ принял участие в [Международной конференции с участием многих заинтересованных сторон по теме "Киберпространство, энергетика и развитие: защита важнейшей энергетической инфраструктуры"](https://www.energypact.org/energypact-foundation_conferences/), организованной правительством Австрии, Фондом EnergyPact и Австрийским технологическим институтом при поддержке МЭК, УНП ООН и МСЭ, которая проходила 16 февраля 2017 года в Вене, Австрия.

6.5 На веб-сайте МСЭ в открытом доступе по-прежнему размещены [195 профилей стран](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx). Профили являются фактическими неаналитическими представлениями состояния кибербезопасности каждой страны на основании [пяти основных составляющих ГПК](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx). Профили представляют собой "живые" документы, которые будут обновляться по мере появления в открытом доступе дополнительной информации по странам.

# 7 Защита ребенка в онлайновой среде (COP)

7.1 Со времени завершения последнего отчетного периода [Рабочая группа Совета по защите ребенка в онлайновой среде](http://www.itu.int/en/council/cwg-cop/Pages/default.aspx) (РГС-COP) провела два собрания, в том числе открытые онлайновые консультации на разные темы с участием молодежи. Дополнительная информация содержится в [Документе C17/15](https://www.itu.int/md/S17-CL-C-0015/en).

7.2 МСЭ и его партнеры продолжают тесно работать для продвижения Целей в области устойчивого развития, особенно ЦУР 16.2 "Положить конец надругательствам, эксплуатации, торговле и всем формам насилия и пыток в отношении детей".

7.3 Во время предыдущих собраний РГС−COP, представитель от Международной линии помощи детям (Child Helpline International − CHI) представил результаты совместной кампании ["Партнерство по защите детей и молодежи"](http://www.itu.int/en/cop/Pages/consultation-may2016.aspx). После начала кампании в мае 2016 года окончательные результаты были представлены 15 ноября 2016 года в ходе Всемирного мероприятия ITU Telecom-2016, а с участниками поделились новыми путями развития служб помощи детям. Особое внимание было уделено сотрудничеству между Членами МСЭ и службами помощи. Члены РГС−COP с удовлетворением отметили эту кампанию, а председатель призвал секретариат продолжить эту работу, с тем чтобы достичь прогресса в контексте ЦУР 16.

7.4 Региональные отделения МСЭ продолжают предоставлять помощь Государствам-Членам в проведении анализа существующей у них среды для защиты ребенка в онлайновой среде, с тем чтобы разработать проект и предложить устойчивую структуру, которая может быть внедрена на длительный срок.

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