|  |  |
| --- | --- |
| **Консультативная группа по развитию электросвязи (КГРЭ)**  **24-е собрание, Женева, 3−5 апреля 2019 года** | C:\Users\comas\AppData\Local\Temp\Rar$DRa0.735\jpg\ITU official logo_blue_RGB.jpg |
|  |  |
|  | **Документ** **TDAG-19/****30-R** |
|  | **25 января 2019 года** |
|  | **Оригинал:** **английский** |
| Директор Бюро развития электросвязи | |
| деятельность В ОБЛАСТИ кибЕРБЕЗОПАСНОСТИ И ПРИЛОЖЕНИЙ ИКТ | |
|  | |
| **Резюме**  В этом отчете представлена обобщенная информация о деятельности в области кибербезопасности и приложений ИКТ – двух намеченных результатах деятельности и целях, которые были приняты Всемирной конференцией по развитию электросвязи в 2017 году (ВКРЭ-17) и подтверждены Полномочной конференцией в 2018 году (ПК-18), соответственно.  С учетом принципов управления, ориентированного на результаты, и направлений действий, в данном отчете представлена обновленная информация о задачах и стратегиях внедрения кибербезопасности и приложений ИКТ, ключевых мероприятиях, которые уже осуществлены или запланированы, а также направлениях дальнейшей деятельности по выполнению задач, связанных с кибербезопасностью.  **Необходимые действия**  КГРЭ предлагается принять к сведению настоящий документ и представить руководящие указания, которые она сочтет необходимыми.  **Справочные материалы**  Декларация Буэнос-Айреса ВКРЭ-17; Резолюции 30 (Пересм. Буэнос-Айрес, 2017 г.), 37 (Пересм. Буэнос-Айрес, 2017 г.), 45 (Пересм. Буэнос-Айрес, 2017 г.), 67 (Пересм. Буэнос-Айрес, 2017 г.), 69 (Пересм. Буэнос-Айрес, 2017 г.); 77 (Пересм. Буэнос-Айрес, 2017 г.), 80 (Пересм. Буэнос-Айрес, 2017 г.) ВКРЭ, Резолюции 130 (Пересм. Дубай, 2018 г.), 139 (Пересм. Дубай, 2018 г.), 179 (Пересм. Дубай, 2018 г.), 197 (Пересм. Дубай, 2018 г.) и 201 (Пересм. Дубай, 2018 г.) ПК | |

# 1 Кибербезопасность

## 1.1 Базовая информация

На всемирных конференциях по развитию электросвязи и полномочных конференциях кибербезопасность в течение многих лет признается одной из важных целей Членов МСЭ.

По итогам ВКРЭ-17 основными задачами МСЭ-D в рамках его мандата в области кибербезопасности является предоставление продуктов и услуг в целях укрепления доверия и безопасности при использовании электросвязи/ИКТ, таких как отчеты и публикации, а также в целях содействия осуществлению национальных и глобальных инициатив.

В намеченном результате деятельности D2-2 Плана действий Буэнос-Айреса (ПДБА) определены пожелания в отношении методов выполнения связанных с кибербезопасностью задач ВКРЭ-17, в частности путем:

− укрепления потенциала Государств-Членов для обмена информацией о киберугрозах, поиска решений для противодействия киберугрозам и реагирования на угрозы кибербезопасности;

− разработки и реализации стратегий и возможностей на национальном уровне;

− создания человеческого и институционального потенциала;

− поощрения национального, регионального и международного сотрудничества в целях расширения взаимодействия Государств‑Членов и соответствующих заинтересованных сторон;

− создания новых партнерств; и

− иной деятельности, которая необходима для выполнения задач, относящихся к кибербезопасности.

## 1.2 Ключевые направления действий и результаты

В рамках программы МСЭ-D в области кибербезопасности осуществляются такие виды деятельности, как подготовка публикаций, проведение национальных и региональных семинаров-практикумов по созданию потенциала, и ведется сотрудничество с партнерами для предоставления высококачественных продуктов и услуг. С момента проведения последнего собрания КГРЭ БРЭ создало несколько новых партнерств для оказания содействия в разработке, осуществлении и реализации проектов и для обмена знаниями и информацией по аналогичным темам на основе консультаций с членами МСЭ и соответствующими основными заинтересованными сторонами. БРЭ также координирует деятельность с другими Секторами и партнерами МСЭ в целях ускорения осуществления различных видов деятельности и реализации инициатив по конкретным ключевым проблемам вместе с соответствующими заинтересованными сторонами.

### 1.2.1 Разработка и обзор стратегии кибербезопасности

[Руководство по национальным стратегиям кибербезопасности](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf), официально представленное на Всемирном мероприятии ITU Telecom-2018, является результатом многосторонних усилий, осуществляемых МСЭ в партнерстве с 11 организациями, среди которых межправительственные и международные организации, представители частного сектора, академические организации и организации гражданского общества. Основная цель этого руководства состоит в том, чтобы страны могли разрабатывать и осуществлять национальные стратегии кибербезопасности, включающие обеспечение готовности к киберугрозам и киберустойчивости. Руководство носит справочный характер и представляет собой всеобъемлющий универсальный ресурс, позволяющий странам получить ясное представление о цели и содержании национальной стратегии кибербезопасности, а также практические рекомендации по разработке собственной стратегии.

### 1.2.2 Программа помощи CIRT

В рамках [Программы CIRT](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx) БРЭ осуществляет несколько видов деятельности, которые обеспечивают конкретные результаты на разных этапах:

− оценка готовности CIRT – целью этой деятельности является обзор имеющейся ситуации в странах, которые проявили интерес к внедрению CIRT, и представление отчета с изложением плана;

− разработка CIRT – целью этого вида деятельности является разработка проектного документа CIRT;

− создание CIRT – базовое и дополнительное обслуживание.

На настоящее время МСЭ провел 75 оценок готовности CIRT и успешно реализовал тринадцать (13) проектов CIRT. На 2019 год планируется создать пять (5) национальных CIRT.

### 1.2.3 Оценка достигнутого прогресса в области кибербезопасности – Глобальный индекс кибербезопасности

В 2018 году были собраны данные по 155 странам для подготовки третьего издания Глобального индекса кибербезопасности. В нем измеряется прогресс стран в области кибербезопасности, что помогает им определить области, в которых необходимы улучшения. Собранная в Глобальном индексе кибербезопасности информация об используемых методах помогает Государствам – Членам МСЭ выявлять пробелы и улучшать те области, которые того требуют.

### 1.2.4 Учения в сфере кибербезопасности (тренировочные занятия по кибербезопасности) – создание потенциала и расширение возможностей

МСЭ проводит региональные и национальные тренировочные занятия по кибербезопасности для Государств – Членов МСЭ. Целью тренировочных занятий по кибербезопасности является улучшение взаимодействия между участвующими группами и дальнейшее совершенствование возможностей реагирования на инциденты, а также поддержание и укрепление национального и международного сотрудничества между странами в деле обеспечения непрерывных коллективных усилий по борьбе с киберугрозами. МСЭ провел двадцать пять (25) тренировочных занятий по кибербезопасности с участием более 100 стран. В 2019 году планируется провести занятия в Европе (Румыния) и Африке (Южно-Африканская Республика). Планируются также занятия в Азиатско-Тихоокеанском регионе, арабских государствах и СНГ. БРЭ изучает возможность межрегионального сотрудничества для двух регионов с целью дальнейшего развития регионального и международного сотрудничества. Учения проводятся совместно с разными партнерами в зависимости от региона.

### 1.2.5 Повышение осведомленности и обмен информацией

БРЭ постоянно выступает в качестве организатора, соорганизатора и участника мероприятий, способствующих повышению осведомленности и обмену информацией. Благодаря различным площадкам и мероприятиям, таким как ВВУИО, собрания исследовательских комиссий и прочие семинары-практикумы, конференции и собрания, БРЭ и партнеры обеспечивают осведомленность и обмениваются информацией. Более подробную информацию о прошедших мероприятиях можно найти на странице с [информацией о мероприятиях](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-events.aspx).

### 1.2.6 Развитие глобальных партнерских отношений и сотрудничества

МСЭ уделяет большое внимание глобальному сотрудничеству и развитию стратегических партнерств в вопросах кибербезопасности. МСЭ способствует выгодной синергии и поддерживает ценные глобальные партнерства с целью повышения кибербезопасности и поощрения запросов на безопасную цифровую среду для всех. Недавно МСЭ создал партнерства, в частности, с ВЭФ и Интерполом.

Партнеры МСЭ в области развития кибербезопасности делятся на группы следующим образом:

− межправительственные организации: например, ЮНИКРИ, ЮНОДК, Содружество, CTO, EC, ENISA и так далее;

− международные организации: FIRST, ISOC, ВЭФ, GFCE, MERIDIAN и так далее;

− частный сектор: Deloitte, Guardtime, Microsoft, HP, Symantec, High-Tech Bridge, Kaspersky и так далее;

− НПО, объединения гражданского общества, академические и благотворительные организации: Индианский университет, Потомакский институт политических исследований, Австралийский институт стратегической политики, Женевский центр по политике безопасности и так далее;

− связанные правительственные и государственные организации: Корейское агентство по развитию интернета и информационной безопасности (KISA), NTRA Египта и другие.

## 1.3 Направления дальнейшей деятельности

БРЭ будет продолжать развитие деятельности в области кибербезопасности путем дальнейшего улучшения результатов в таких областях, как:

− дальнейшее оказание технической помощи Государствам-Членам посредством инноваций и новых продуктивных партнерских отношений;

− более активная реализация проектов и осуществление видов деятельности, связанных с созданием человеческого и институционального потенциала;

− приоритетность реализации проектов и инициатив с высокой отдачей, таких как деятельность в рамках национальной программы CIRT, разработка и обзор национальной политики в области кибербезопасности и так далее;

− дальнейшая оценка достигнутого прогресса в области кибербезопасности с помощью Глобального индекса кибербезопасности и одновременное совершенствование методики и механизма оценки путем постоянного диалога и сотрудничества с Государствами-Членами, компаниями отрасли, академическими организациями и экспертами в области кибербезопасности и анализа данных;

− дальнейшая разработка направлений и развитие кибербезопасности в области электросвязи/ИКТ, в том числе ИИ/ML, большие данные, IoT, 5G, ESIM и так далее.

# 2 Приложения ИКТ

## 2.1 Базовая информация

Как на всемирных конференциях по развитию электросвязи (ВКРЭ-14 и ВКРЭ-17), так и на полномочных конференциях (ПК-14 и ПК-18) Члены МСЭ признали, что в наше время наиболее мощной преобразующей силой обладают электросвязь/ИКТ и в особенности технологии подвижной связи. С их помощью возможно подсоединить даже самые изолированные сообщества к источникам информации и услугам, непосредственно воздействующим на их средства к существованию и качество жизни.

В свете сохраняющейся актуальности Направлений деятельности ВВУИО, а также принятия новых Целей в области устойчивого развития обязательным условием их достижения к 2030 году является включение аспекта цифровых инноваций в деятельность всех секторов.

В соответствии с решениями ВКРЭ-14 и ВКРЭ-17, основные задачи Программы МСЭ-D в области услуг и приложений ИКТ заключаются в оказании поддержки Членам МСЭ при сотрудничестве и в партнерстве с другими организациями системы Организации Объединенных Наций и частным сектором в стимулировании использования электросвязи/ИКТ для различных аспектов развития информационного общества, в частности в недостаточно обслуживаемых и сельских районах, в целях устойчивого развития и достижения Целей в области устойчивого (ЦУР) ООН и реализации Направлений деятельности Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО).

Программа ориентирована на обеспечение продуктами и услугами, связанными с политикой в сфере электросвязи/ИКТ, которая содействует развитию цифровой экономики, приложений ИКТ и новых технологий, такие как обмен информацией и поддержка их развертывания, аналитические исследования и комплекты материалов по приложениям ИКТ (Намеченный результат деятельности 4.2).

## 2.2 Ключевые направления действий и результаты

В 2018 году БРЭ провело работу по ряду ключевых направлений, а именно:

Поддержка разработки национальных основ стратегического планирования, способствующих становлению цифровой экономики, и соответствующих комплектов материалов

Одной из основных задач программы "Приложения ИКТ" является оказание содействия странам в разработке национальных электронных стратегий. Эти национальные электронные стратегии по сути обеспечивают концептуальный проект и дорожную карту для цифровой трансформации секторов.

В секторе здравоохранения совместное Руководство МСЭ–ВОЗ по национальной стратегии электронного здравоохранения, опубликованное в 2012 году, стало эталоном с точки зрения разработки стратегии цифрового здравоохранения. Им воспользовались во многих странах и почти во всех регионах мира. В 2018 году поддержка, в том числе поддержка МСЭ и ВОЗ, была оказана таким странам, как Сенегал, Бенин, Мадагаскар, Нигер и Лесото.

В сфере сельского хозяйства в нескольких странах, таких как Филиппины, Шри-Ланка, Бутан, Фиджи, Папуа-Новая Гвинея, уже воспользовались разработанным МСЭ в сотрудничестве с ФАО Руководством по национальной стратегии в области электронного сельского хозяйства. В настоящее время Руководство при содействии МСЭ и ФАО используют Бенин, страны Карибского бассейна, Пакистан и Афганистан.

БРЭ в сотрудничестве с ЮНЕСКО проводит обзор Политики "умного" обучения для Судана.

В целом эти стратегии предоставляют стране комплекс мероприятий, необходимых для инициирования и поддержания процесса секторальных (или межсекторальных) преобразований с использованием цифрового инструментария.

В 2019 году в рамках программы "Приложения ИКТ" для Папуа-Новой Гвинеи будет разрабатываться Генеральный план электронного правительства с использованием недавно разработанной Структуры цифровых инвестиций для ЦУР, которая была подготовлена вместе с Альянсом по вопросам воздействия цифровых технологий (DIAL).

Содействие развертыванию приложений ИКТ/мобильных приложений в целях улучшения предоставления услуг с добавленной стоимостью в обладающих высоким потенциалом областях, таких как электронное здравоохранение, включая мобильное здравоохранение, образование, сельское хозяйство

Кроме того, в рамках программы "Приложения ИКТ" ведется сотрудничество со странами в целях поддержки реализации этих стратегий путем осуществления таких проектов, как разработка приложений для отслеживания свиней на основе блокчейн-технологий в Папуа-Новой Гвинее, запуск нескольких проектов в рамках Совместной программы МСЭ−ВОЗ "Мобильное здравоохранение для борьбы с неинфекционными заболеваниями" ("Будь здоровым, будь мобильным"), развертывание "умных" деревень в Нигере и так далее. В рамках этой программы страны, например Лесото, получают помощь в подготовке подробных технических требований к разработке собственной национальной архитектуры предприятий в сфере цифрового здравоохранения и структуры функциональной совместимости на основе собственной национальной стратегии электронного здравоохранения.

Разработка подробных исследований и содействие обмену знаниями и передовым опытом

Помимо поддержки разработки стратегий, деятельность направлена на создание потенциала для национальных лидеров в области цифрового здравоохранения. Например, в Лесото в 2018 году был проведен региональный семинар-практикум по потенциалу цифрового здравоохранения для 12 африканских стран. Все представленные материалы и контент записаны и будут размещены на онлайновой платформе электронного обучения. Еще один семинар-практикум для франкоязычных стран запланирован на 2019 год.

Был проведен ряд мероприятий по обмену знаниями, среди которых посвященный здравоохранению сегмент, проведенный в рамках Саммита "ИИ для здравоохранения"; посвященный ликвидации голода хакатон, проведенный совместно с ФАО во время Форума ВВУИО; форум по решениям в области электронного сельского хозяйства, проведенный совместно с ФАО в Китае. Кроме того, был опубликован отчет об использовании дронов в сельском хозяйстве в дополнение к нескольким справочникам, подготовленным совместно с ВОЗ, по использованию мобильного здравоохранения в вопросах старения, прекращения употребления табака, рака шейки матки, диабета и респираторных заболеваний.

## 2.3 Направления дальнейшей деятельности

В рамках программы "Приложения ИКТ" будут и далее укрепляться такие направления, как:

− дальнейшее создание потенциала в сфере разработки цифровой стратегии и решений путем проведения национальных и региональных семинаров-практикумов по созданию потенциала;

− разработка новых инструментов для содействия правительствам на пути цифровой трансформации, таких как разработка архитектуры государственного предприятия;

− поддержка разработки страновых планов и технических исследований по вопросам отраслевой и межотраслевой цифровой трансформации;

− продвижение и поддержка межсекторальных и общегосударственных подходов к эффективному расширению масштабов внедрения цифровых инструментов.

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