



Бюро развития  
электросвязи (BDT)



Осн.: BDT/DNS/СУВ

Женева, 10 августа 2021 года

- Государствам – Членам МСЭ
- Членам Сектора МСЭ-D
- Академическим организациям – Членам МСЭ
- Региональным/международным организациям
- CERT основных отраслей национальной экономики/национальным CERT
- Координаторам МСЭ по вопросам кибербезопасности

**Предмет: Приглашение принять участие в глобальном тренировочном занятии МСЭ по кибербезопасности 2021 года**

Уважаемая госпожа,  
Уважаемый господин,

Имею честь пригласить вас принять участие в организуемом Международным союзом электросвязи (МСЭ) глобальном тренировочном занятии по кибербезопасности 2021 года, которое будет проводиться с сентября по ноябрь. Аналогично тренировочному занятию по кибербезопасности 2020 года, вместо региональных тренировочных занятий МСЭ по кибербезопасности будет проведено единое тренировочное занятие в виртуальном формате.

В рамках работы тренировочного занятия по кибербезопасности 2021 года особое внимание будет уделяться роли национальных групп реагирования на компьютерные инциденты (CIRT) и групп реагирования на инциденты в сфере компьютерной безопасности (CSIRT) в формировании способности к восстановлению в киберсреде и в защите критической информационной инфраструктуры; тематическими концепциями тренировочного занятия по кибербезопасности 2021 года являются *анализ, обмен, обучение и опыт*.

Данное виртуальное тренировочное занятие послужит платформой для развития потенциала для целей улучшения существующих механизмов связи и укрепления инновационных подходов к сотрудничеству для национальных CIRT/CSIRT. В рамках мероприятия состоятся межрегиональные собрания, вебинары, технические учебные занятия, тренировочные занятия по кибербезопасности, а также будет представлена возможность для налаживания связей между группами по кибербезопасности из Государств – Членов МСЭ, Членов Секторов, включая академические организации, региональные и международные организации, операторов электросвязи, регуляторные органы и другие заинтересованные стороны.

Рекомендуется, чтобы участвующие организации представляли группы, состоящие как минимум из двух (2) технических специалистов и одного (1) сотрудника руководящего звена. Дополнительная информация содержится в круге ведения (см. Приложение 1), а также на веб-сайте мероприятия: <https://itu.int/go/GCD2021>.

По всем вопросам, связанным с глобальным тренировочным занятием МСЭ по кибербезопасности этого года, просьба обращаться к ответственным за тематические приоритетные направления по кибербезопасности в региональных отделениях МСЭ; подробная информация содержится в Приложении.

Надеюсь на ваше участие в этом виртуальном тренировочном занятии по кибербезопасности.

С уважением,

[Оригинал подписан]

Дорин Богдан-Мартин  
Директор



**Программа МСЭ/БРЭ в области  
кибербезопасности**

**Глобальное тренировочное занятие МСЭ  
по кибербезопасности 2021 года**

**Круг ведения**

Июль 2021 года

## Круг ведения

### 1 ВВЕДЕНИЕ

Международный союз электросвязи (МСЭ) стремится расширять возможности Государств-Членов по обеспечению готовности к кибербезопасности, информационной безопасности, а также по реагированию на инциденты путем организации на национальном, региональном и глобальном уровнях тренировочных занятий по кибербезопасности. В рамках таких ежегодных мероприятий выполняется моделирование кибератак, инцидентов информационной безопасности и нарушений других типов, для того чтобы проверить возможности организации в области кибербезопасности. За последние десять лет МСЭ провел более тридцати тренировочных занятий в партнерстве с более чем 100 странами, стремящимися повысить уровень кибербезопасности на национальном и глобальном уровнях.

Как правило, тренировочные занятия МСЭ проводятся на региональном уровне, однако мероприятия 2020 и 2021 годов объединяют сообщество кибербезопасности и, в частности, Государства – Члены МСЭ на глобальном уровне для решения проблем, вызванных пандемией COVID-19.

Работа глобального тренировочного занятия 2021 года будет основываться на обсуждениях и результатах прошлогоднего мероприятия; основное внимание будет уделено роли национальных групп по реагированию на компьютерные инциденты (CIRT) и групп по реагированию на инциденты компьютерной безопасности (CSIRT) в формировании способности к восстановлению в киберсреде и в защите критической информационной инфраструктуры.

### 2 ЦЕЛИ

Сессии в рамках глобального тренировочного занятия 2021 года будут организованы в соответствии с четырьмя тематическими концепциями: *анализ, обмен, обучение и опыт*.

- **Анализ:** сбор глобального кибербезопасности региональных кибербезопасности возможностей пяти основных программы (ГПК) МСЭ и кибербезопасности
- **Обмен:** содействие рамках полезной информацией о финансировании.
- **Обучение:** создание CSIRT в области инциденты и защиты информационной инфраструктуры (CIIP).
- **Опыт:** проверка ключевых принципов эксплуатационной устойчивости во всем сообществе CSIRT/CIRT/CERT.



представителей сообщества для анализа основных тенденций в области и рассмотрения улучшения на основе элементов Глобальной кибербезопасности Глобального индекса (GCI).

обмену знаниями в сетях связи и обмену ресурсами источников

потенциала сообществ реагирования на критической

### 3 ПРЕДУСМОТРЕННЫЕ МЕРОПРИЯТИЯ

Все мероприятия тренировочного занятия по кибербезопасности будут проводиться в виртуальном формате в течение трех месяцев. Эксперты МСЭ в сотрудничестве с партнерами в этой области организуют и/или проведут нижеследующие мероприятия.

- **Три (3) межрегиональных собрания (Анализ):** в рамках собраний выступят руководители структур, занимающихся вопросами кибербезопасности, из правительственных органов, региональных организаций и т. д., которые поделятся передовым опытом и извлеченными уроками в области защиты критической информационной инфраструктуры (CIIP).
  - **Межрегиональное собрание I:** Азиатско-Тихоокеанский регион и Регион СНГ.
  - **Межрегиональное собрание II:** Регионы Африки и Европы.
  - **Межрегиональное собрание III:** Регионы Северной и Южной Америки и арабских государств.
- **Два (2) вебинара (Обмен):**
  - **Вебинар I:** Раскрытие потенциала сотрудничества в области кибербезопасности: возможности, проблемы и дальнейшие шаги. Докладчики осветят огромный объем ресурсов, доступных сообществу CSIRT, в частности, механизмы финансирования в рамках международных организаций.
  - **Вебинар II:** Женщины в сфере кибербезопасности: год спустя.  
 В 2021 году МСЭ приступил к реализации программы наставничества "Женщины в сфере кибербезопасности" (в сотрудничестве с Форумом по реагированию на инциденты и группам безопасности (FIRST) и партнерством "РАВНЫЕ"). Программа подготовлена по итогам вебинара "Расширение прав и возможностей женщин в сфере кибербезопасности", состоявшегося в рамках тренировочного занятия по кибербезопасности 2020 года, на котором была выявлена необходимость в примерах для подражания и наставничестве, что является важнейшим фактором для увеличения числа женщин на руководящих постах в области кибербезопасности. Программа основана на текущих усилиях МСЭ по сокращению цифрового гендерного разрыва путем выдвижения на первый план ориентированных на гендерные вопросы мероприятий, привлекает примеры для подражания и руководителей в этой области и связывает их с перспективными женщинами во всем мире.  
 Первый этап программы был успешно реализован, и в работе сессии примут участие наставники, подопечные и инструкторы, чтобы обсудить результаты работы программы, поделиться впечатлениями и передовым опытом в рамках совместных усилий по определению перспектив программы и сообщества на 2022 год и последующий период.
- **Шесть (6) учебных сессий (Обучение):** эксперты МСЭ совместно с партнерскими организациями проведут учебные занятия во второй половине мероприятия. Блоки учебных занятий пройдут в течение трех недель и будут посвящены следующим темам:
  - Определение и классификация объектов и услуг критической информационной инфраструктуры.
  - Укрепление правовой и политической базы и системы соблюдения требований для CIIP.
  - Отслеживание угроз и реагирование на инциденты с участием CNI с использованием инструментов с открытым исходным кодом.
  - Основы защиты от DDoS-атак.
  - Проведение упражнений для совершенствования способности реагировать на инциденты.
  - Измерение и повышение уровня развития национальной CIRT.
- **Шесть (6) упражнений на основе сценариев (Опыт):** упражнения являются одним из основных элементов тренировочного занятия МСЭ и открыты для национальных/правительственных CIRT/CSIRT. Участвующие страны представлены группами из двух-четырёх человек; упражнения проводятся в течение двух недель.

Три межрегиональных собрания будут открыты только для Государств-Членов из данного конкретного региона. Остальные вебинары, учебные занятия и упражнения на основе сценариев будут открыты для всех участников, независимо от региона.

#### 4 ЦЕЛЕВАЯ АУДИТОРИЯ

Региональные диалоги, вебинары и учебные занятия открыты для представителей национальных CIRT/CSIRT, министерств, регуляторных органов, операторов электросвязи, академических организаций и образовательных учреждений, производителей оборудования электросвязи, научно-исследовательских и проектных институтов, разработчиков программного обеспечения и других заинтересованных сторон Государств – Членов МСЭ и Членов Секторов МСЭ.

#### 5 РЕГИСТРАЦИЯ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Всем участникам мероприятий тренировочного занятия по кибербезопасности рекомендуется иметь компьютер или ноутбук с устойчивым интернет-соединением.

С дополнительной информацией о тренировочном занятии по кибербезопасности 2021 года можно ознакомиться на веб-сайте мероприятия: <https://itu.int/go/GCD2021>.

Подробная информация для регистрации, в том числе ссылки на собрания и дополнительная информация о собраниях, будет направлена по зарегистрированным адресам электронной почты участников. Регистрация для участия в учебных занятиях и упражнениях закроется в среду, 10 сентября 2021 года, или когда будут забронированы все места на сессиях.

#### 6 КОНТАКТНЫЕ ДАННЫЕ

По любым вопросам просим обращаться к региональным координаторам МСЭ по вопросам кибербезопасности:

- Региональное отделение для Африки: г-н Серж Валери Зонго ([serge.zongo@itu.int](mailto:serge.zongo@itu.int));
- Региональное отделение для Северной и Южной Америки: г-н Пабло Паласиос ([Pablo.Palacios@itu.int](mailto:Pablo.Palacios@itu.int));
- Региональное отделение для арабских государств: г-н Ахмед Эль-Раги ([ahmed.elraghy@itu.int](mailto:ahmed.elraghy@itu.int));
- Региональное отделение для Азиатско-Тихоокеанского региона: г-н Калвин Чэн ([calvin.chan@itu.int](mailto:calvin.chan@itu.int));
- Региональное отделение для СНГ: г-н Фарид Нахли ([farid.nakhli@itu.int](mailto:farid.nakhli@itu.int));
- Региональное отделение для Европы: г-н Ярослав Пондер ([jaroslaw.ponder@itu.int](mailto:jaroslaw.ponder@itu.int)).

#### 7 КАЛЕНДАРЬ МЕРОПРИЯТИЙ

Регулярные обновления повестки дня будут публиковаться на веб-странице тренировочного занятия по кибербезопасности. Для получения подробной и актуальной информации просим обращаться к онлайн-календарю по адресу: <https://itu.int/go/GCD2021>.

