Бюро развития электросвязи
(BDT)

Осн.: Циркуляр/BDT/DNS/CYB/051 Женева, 24 июля 2020 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 2020 года

Уважаемая госпожа/
уважаемый господин,

Имею честь пригласить вас принять участие в организуемом Международным союзом электросвязи (МСЭ) глобальном тренировочном занятии по кибербезопасности 2020 года, которое будет проводиться с сентября по ноябрь 2020 года. Вследствие продолжающейся пандемии COVID-19 и связанных с ней рисков и ограничений в отношении поездок и собраний, тренировочное занятие МСЭ по кибербезопасности будет проведено в виртуальном формате.

Пандемия COVID-19 привела к росту во всем мире уровня использования информационно-коммуникационных технологий (ИКТ). ИКТ обеспечили для людей возможность эффективной деятельности и участия даже в условиях социального дистанцирования. Такой возросший уровень использования ИКТ создал также и значительные проблемы кибребезопасности, вызванные ростом киберугроз.

Запланированные на 2020 год региональные тренировочные занятия МСЭ по кибербезопасности будут заменены одним виртуальным глобальным тренировочным занятием по кибербезопасности. В рамках глобального тренировочного занятия по кибербезопасности мы организуем в течение трех (3) месяцев серию региональных диалогов, международных вебинаров, учебных сессий и упражнений на основе сценариев, с тем чтобы оказать помощь в создании в странах потенциала для более эффективной борьбы с киберугрозами. Подробная информация содержится в информационных материалах о мероприятиях, прилагаемых к настоящему письму (Приложение 1).

Глобальное тренировочное занятие по кибербезопасности – это мероприятие по созданию потенциала, которое направлено на расширение возможностей участвующих групп по обмену информацией и реагированию на инциденты, а также содействие коллективным усилиям национальных групп реагирования на компьютерные инциденты (CIRT) и групп реагирования на инциденты в сфере компьютерной безопасности (CSIRT).

Участие в тренировочном занятии по кибербезопасности могут принять группы представителей национальных CIRT/CSIRT, министерств, регуляторных органов, операторов электросвязи, высших учебных заведений и образовательных учреждений, производителей оборудования электросвязи, научно-исследовательских и проектных институтов, разработчиков программного обеспечения и других заинтересованных сторон Государств – Членов МСЭ, Членов Секторов МСЭ и Академических организаций – Членов МСЭ. Рекомендуется, чтобы участвующая группа состояла как минимум из двух (2) технических специалистов и одного (1) сотрудника руководящего звена.

Для получения дополнительной информации и регистрации для участия в мероприятиях глобального тренировочного занятия по кибербезопасности воспользуйтесь ссылкой: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx.

По всем вопросам, связанным с мероприятиями в рамках Глобального тренировочного занятия МСЭ по кибербезопасности 2020 года, просьба обращаться к ответственным за тематические приоритетные направления по кибербезопасности в региональных отделениях МСЭ:

- Региональное отделение для Африки: г-н Серж Валери Зонго (serge.zongo@itu.int);
- Региональное отделение для Северной и Южной Америки: г-н Пабло Паласиос (Pablo.Palacios@itu.int);
- Региональное отделение для арабских государств: г-жа Руда Аламир Али (Rouda.AlamirAli@itu.int);
- Региональное отделение для Азиатско-Тихоокеанского региона: г-н Самир Шарма, (sameer.sharma@itu.int);
- Региональное отделение для СНГ: г-н Фарид Нахли (farid.nakhli@itu.int);
- Региональное отделение для Европы: г-н Ярослав Пондер (jaroslaw.ponder@itu.int).

С уважением,

[оригинал подписан]

Дорин Богдан-Мартин,
Директор

ПРИЛОЖЕНИЕ 1

Глобальное тренировочное занятие МСЭ по кибербезопасности 2020 года

1 ВВЕДЕНИЕ

Международный союз электросвязи (МСЭ), организуя на региональном и международном уровнях тренировочные занятия по кибербезопасности, расширяет возможности Государств-Членов по обеспечению готовности к кибербезопасности, информационной безопасности, а также по реагированию на инциденты. Тренировочное занятие по кибербезопасности – это ежегодное мероприятие, в ходе которого выполняется моделирование кибератак, инцидентов информационной безопасности и нарушений других типов, для того чтобы проверить возможности организации в области кибербезопасности: от способности обнаружить инцидент в области безопасности до способности надлежащим образом реагировать на него и минимизировать любое связанное с ним воздействие. Участники тренировочного занятия по кибербезопасности могут проверять стратегии, планы, процедуры, процессы и возможности, обеспечивающие подготовку, предотвращение, реагирование, восстановление и непрерывность деятельности. К настоящему времени МСЭ провел по всему миру более 29 тренировочных занятий по кибербезопасности, цель которых заключается в повышении потенциала и расширении возможностей в области кибербезопасности путем регионального сотрудничества и взаимодействия.

2 ЦЕЛИ

Основные цели данного тренировочного занятия по кибербезопасности:

- обеспечение информированности о ситуации ключевых участников государственного и частного секторов, которые выполняют руководящие функции в своих компаниях, организациях или юрисдикциях в условиях нарушения кибербезопасности;
- объединение сообщества CERT/CIRT/CSIRT в рамках единого учебного мероприятия для создания глобальных возможностей по реагированию и восстановлению;
- проверка ключевых принципов эксплуатационной устойчивости во всем сообществе CSIRT/CIRT/CERT;
- определение, осуществление и содействие совершенствованию процессов, процедур, механизмов взаимодействия и обмена информацией, которые существуют или должны существовать в CERT/CSIRT, SOC, учреждениях, государственных органах, а также в региональных организациях, ответственных за управление в кризисных ситуациях, и регуляторных органах;
- использование механизмов координации, выполнение обмена информацией, разработка процедур общей информированности о ситуации, а также принятия решений сообщества кибербезопасности в ходе мероприятий по кибербезопасности;
- повышение уровня осведомленности о других инициативах в области кибербезопасности.

3 ПРЕДУСМОТРЕННЫЕ МЕРОПРИЯТИЯ

Вследствие ограничений на поездки и других значительных мер, принятых в ответ на пандемию COVID-19, мероприятия тренировочного занятия по кибербезопасности будут проводиться в онлайновом режиме в течение трех (3) месяцев – с сентября по ноябрь 2020 года. Эксперты МСЭ в сотрудничестве с партнерами в этой области организуют и/или проведут нижеследующие мероприятия.

- **Шесть (6) региональных диалогов, которые посвящены урокам, извлеченным из пандемии COVID-19**

  a) Пандемия COVID-19 увеличила нагрузку на национальные системы ИКТ, в некоторых случаях сделав их более уязвимыми для кибератак на важнейшую инфраструктуру.

Региональные диалоги обеспечат возможность представителям CSIRT/CIRT/CERT всех Государств-Членов обменяться своим опытом решения проблем кибербезопасности в условиях пандемии COVID-19.

- **Три (3) вебинара**

  a) **Расширение прав и возможностей женщин в сфере кибербезопасности**: участники этого вебинара обсудят роль женщин в сфере кибербезопасности во всех секторах. Эта серия мероприятий будет открыта для всех участников.

  b) **Управление в условиях киберкризиса**: наличие специальной стратегии управления в условиях киберкризиса является основой для формирования национальной киберустойчивости. В данной группе будут представлены эксперты по управлению в условиях киберкризиса. Эта серия мероприятий будет открыта для всех участников.

  c) **Измерение и повышение уровня зрелости CIRT**: это групповое обсуждение будет посвящено измерению и повышению уровня зрелости как важнейшим аспектам непрерывного развития и укрепления возможностей CSIRT. В данном вебинаре примут участие эксперты, имеющие обширный опыт работы с CIRT. Эта серия мероприятий будет открыта для всех участников.

- **Шесть (6) учебных сессий**

  a) Эти учебные сессии проведут эксперты МСЭ в сотрудничестве с организациями-партнерами, и каждая из них состоится в разные дни и в заранее определенное время. На учебных сессиях будут обсуждаться такие вопросы, как создание эффективного потенциала для сбора оперативной информации о киберугрозах (CTI), реагирование на инциденты, связь при управлении в условиях кризиса, промышленная кибербезопасность и реагирование на инциденты, определение ложной информации и практический анализ киберугроз. Эти учебные сессии будут открыты для всех участников.

- **Шесть (6) упражнений на основе сценариев**

  a) Проведение упражнений на основе сценариев – одна из основных особенностей тренировочного занятия МСЭ по кибербезопасности. В нынешнем году МСЭ планирует провести шесть упражнений на основе сценариев в различные дни и в определенное время. Участие в упражнениях могут принять только представители национальных/правительственных CIRT/CSIRT, и каждая участвующая страна будет представлена одной группой в составе не менее двух (2) и не более четырех (4) участников.

Региональные вебинары "CIRT и уроки, извлеченные из кризиса COVID-19" 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

Участие в региональных диалогах, вебинарах и учебных занятиях могут принять представители 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.

Участие в упражнениях могут принять только представители национальных/правительственных CIRT/CSIRT, и каждая зарегистрированная страна будет представлена одной группой в составе двух (2) участников.

5 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Мы рекомендуем всем участникам мероприятий тренировочного занятия по кибербезопасности иметь компьютер или ноутбук с устойчивым и подходящим интернет-соединением.

6 РЕГИСТРАЦИЯ

Для получения дополнительной информации и регистрации для участия в мероприятиях просим обращаться на веб-сайт мероприятия: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx.

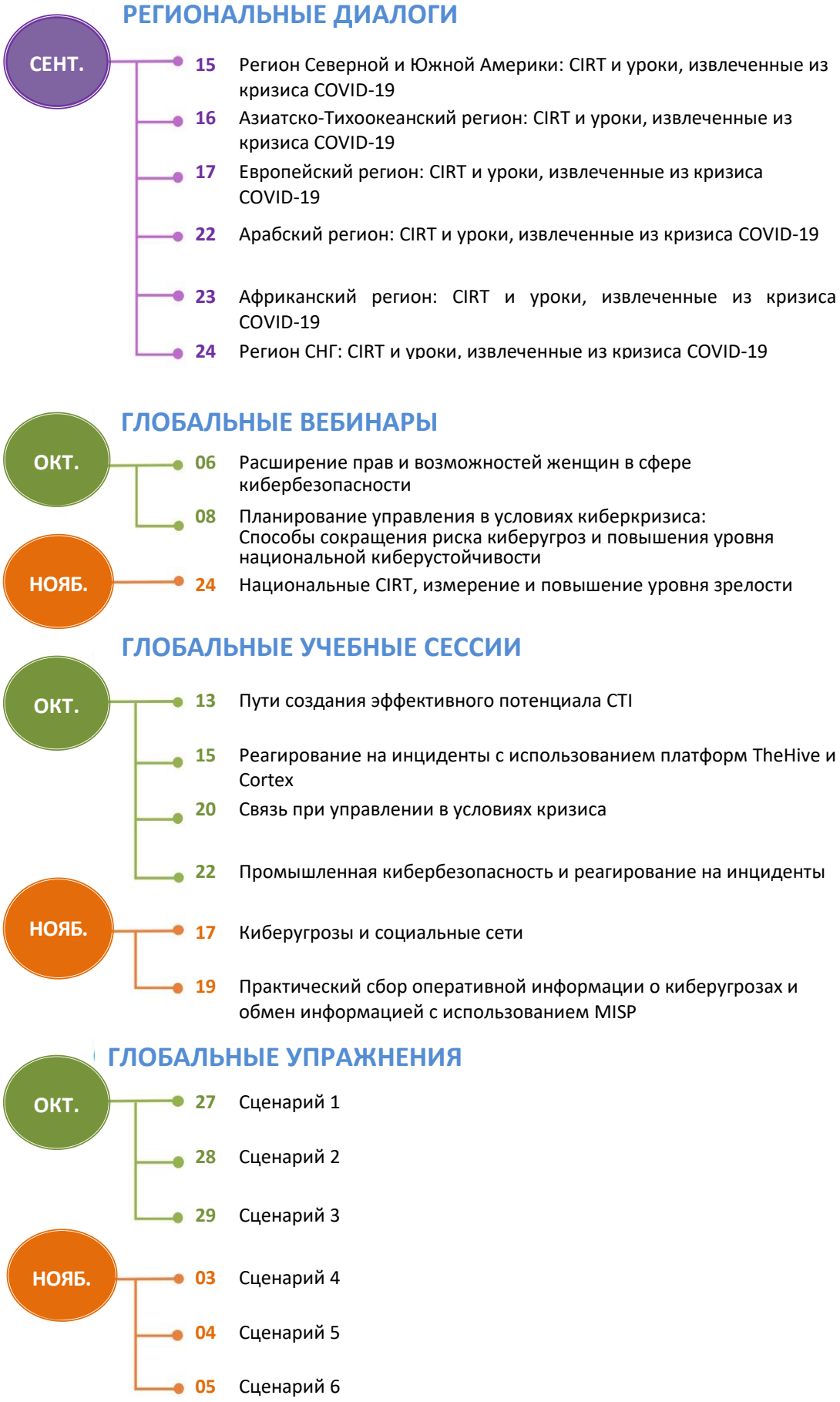
Сведения для регистрации, включая ссылки на собрания и другую информацию, будут направлены по зарегистрированным адресам электронной почты участников. Регистрация для участия в учебных занятиях и упражнениях закроется в среду, 30 сентября 2020 года, или когда будут забронированы все места на сессиях.

7 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);
- Региональное отделение для Северной и Южной Америки: г-н Пабло Паласиос (Pablo.Palacios@itu.int);
- Региональное отделение для арабских государств: г-жа Руда Аламир Али (Rouda.AlamirAli@itu.int);
- Региональное отделение для Азиатско-Тихоокеанского региона: г-н Самир Шарма, (sameer.sharma@itu.int);
- Региональное отделение для СНГ: г-н Фарид Нахли (farid.nakhli@itu.int);
- Региональное отделение для Европы: г-н Ярослав Пондер (jaroslaw.ponder@itu.int).

8 КАЛЕНДАРЬ МЕРОПРИЯТИЙ



Регулярные обновления повестки дня будут публиковаться на веб-странице тренировочного занятия по кибербезопасности. Для получения подробной и актуальной информации просим обращаться к онлайновому календарю по адресу: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx.