



Пресс-релиз

## "ALERT МСЭ-ИМПАКТ 2011"

### В Юго-Восточной Азии проводится новаторское тренировочное занятие по кибербезопасности

**Женева, 2 декабря 2011 года** – Международный союз электросвязи (МСЭ), являющийся специализированным учреждением системы Организации Объединенных Наций, и Международное многостороннее партнерство против киберугроз (ИМПАКТ) провели вчера первое в мире трансграничное тренировочное занятие, которое было организовано международной организацией и учреждением Организации Объединенных Наций.

Первое тренировочное занятие по кибербезопасности было проведено в рамках ALERT (практическое обучение для группы реагирования на случаи чрезвычайных ситуаций) МСЭ-ИМПАКТ и включало смоделированные ответные меры на кибератаку, предусматривающие связь Группы реагирования на нарушения компьютерной защиты/Группы реагирования на компьютерные инциденты (CERT/CIRT) Камбоджи, Лаосской Народно-Демократической Республики, Мьянмы и Вьетнама (страны КЛМВ) с выполняющими соответствующие функции специалистами МСЭ-ИМПАКТ. Однодневное тренировочное занятие состоялось в связи с субрегиональным семинаром CSIRT/CIRT/CERT МСЭ-АСЕАН для стран КЛМВ в Янгоне, Мьянма.

ИМПАКТ, исполнительная структура по кибербезопасности МСЭ, является крупнейшим объединением подобного рода в мире, насчитывающим 137 стран-партнеров, формально являющихся в настоящее время частью коалиции МСЭ-ИМПАКТ, – объединением, пользующимся твердой поддержкой глобальных отраслевых гигантов, партнеров из числа академических и международных организаций.

Тренировочное занятие по кибербезопасности являлось смоделированным и скоординированным учебным мероприятием, предназначенным для оценки готовности к чрезвычайным ситуациям в области кибербезопасности стран КЛМВ и их возможностей реагирования на инциденты при смягчении последствий кибератак и противодействии им. Это учебное мероприятие помогло наладить более тесное международное сотрудничество между участвующими странами, усовершенствовать их связь и процедуры смягчения последствий. Его уникальность заключалась также в том, что оно было специально предназначено для стран с различными статусами развития: одна быстрорастущая развивающаяся страна (Вьетнам) и три страны, относящиеся к наименее развитым странам, согласно классификации ООН, – Камбоджа, Лаосская Народно-Демократическая Республика и Мьянма. Это означало, что данное тренировочное занятие было способно учесть реальные ограничения, с которыми сталкиваются многие развивающиеся страны.

Важным аспектом тренировочного занятия стало участие в нем стран на региональном уровне. "Кибератаки не имеют границ, и поэтому для каждой CERT/CIRT важно обмениваться информацией и опытом в области урегулирования трансграничных инцидентов, для того чтобы отработать и проверить точки соприкосновения и соответствующие процедуры, в целях повышения эффективности их мер по реагированию на киберугрозы", – сказал Генеральный секретарь МСЭ д-р Хамадун Туре.

В тренировочном занятии приняли участие группы от каждой из четырех стран КЛМВ. Сценарии тренировочного занятия включали три инцидента чрезвычайной ситуации в области кибербезопасности: **массированное искажение внешнего вида веб-сайта, спам и заражение вредоносной программой**. Группы должны были определить происхождение атак, наметить возможные решения, меры по смягчению последствий и исправить такое искажение/или вторжение. Все события и инциденты были смоделированы без атаки на работающие системы.

Все группы участвующих стран были поделены на две части с отведением им соответствующих ролей, отражая "участника" и "наблюдателя". Участник осуществлял процесс управления инцидентом, анализировал угрозы и смягчал последствия атак, в то время как наблюдатель осуществлял функции связи и помогал участнику смягчить последствия смоделированных атак.

Сценарии тренировочного занятия были разработаны специалистами МСЭ-ИМПАКТ, F-Secure и Trend Micro. Хотя они и являются конкурентами во внешнем мире, давняя традиция МСЭ по установлению партнерских отношений между государственным и частным секторами позволила создать уникальную платформу для этих партнеров, с тем чтобы объединиться в интересах мирового сообщества в целях повышения готовности противодействовать кибератакам.

Это тренировочное занятие было проведено как учебное мероприятие "без отказа" системы. Его цель заключалась не в том, чтобы критиковать возможности, ту или иную конкретную сеть, систему или инфраструктуру, а в том, чтобы обратить внимание на необходимость наличия каналов постоянной связи между соседними странами и усиления возможностей реагирования на инциденты в каждой стране.

"ALERT МСЭ-ИМПАКТ позволила выявить некоторые позитивные результаты, включая определение готовности группы CERT/CIRT каждой страны, выявление потребности в наличии надлежащих планов действия в чрезвычайных ситуациях, лучшую осведомленность в отношении средств и другого соответствующего программного обеспечения и информирование о важности ведения журналов и наличия надлежащим образом подготовленного персонала, способного управлять киберугрозами", – сказал Датук Мохд Нур Амин, Председатель ИМПАКТ. "Это стало хорошей возможностью для стран на практике проверить свои стратегии действий в чрезвычайных ситуациях. Это тренировочное занятие по кибербезопасности служит прототипом для предстоящих более крупных глобальных тренировочных занятий, которые планируются провести в 2012 году", – добавил он.

"ALERT МСЭ-ИМПАКТ" 2011 года было организовано при спонсорской поддержке ABI research и технической помощи со стороны Trend Micro и F-Secure.

**Дополнительную информацию можно получить, обратившись к:**

#### **В МСЭ**

##### **Марко Обисо (Marco Obiso)**

Координатор МСЭ по вопросам кибербезопасности

Тел.: +41 22 730 6760;

моб. тел.: +41 79 217 3590;

эл. почта: [marco.obiso@itu.int](mailto:marco.obiso@itu.int)

##### **Сара Паркес (Sarah Parkes)**

Руководитель Отдела связей со СМИ и общественной информации

Тел.: +41 22 730 6039;

моб. тел.: +41 79 599 1439;

эл. почта: [pressinfo@itu.int](mailto:pressinfo@itu.int)

#### **В ИМПАКТ**

##### **Кала Пакири (Kala Pakiri)**

Руководитель Отдела корпоративной связи

Тел.: +60 3 8313 2124;

эл. почта: [kalaivani.pakiri@impact-alliance.org](mailto:kalaivani.pakiri@impact-alliance.org)

## **Об МСЭ**

МСЭ является ведущим учреждением Организации Объединенных Наций в области информационно-коммуникационных технологий. На протяжении более 145 лет МСЭ осуществляет на глобальной основе координацию совместного использования радиочастотного спектра, содействует международному сотрудничеству при распределении орбитальных позиций для спутников, способствует совершенствованию инфраструктуры электросвязи в развивающихся странах и создает всемирные стандарты, которые обеспечивают беспрепятственное взаимодействие широкого диапазона систем связи. От широкополосных сетей до беспроводных технологий нового поколения, воздушной и морской навигации, радиоастрономии, метеорологии с использованием спутников и конвергенции фиксированной и мобильной телефонной связи, интернета и технологий радиовещания – все это свидетельствует о том, что МСЭ верен идее соединить мир.

[www.itu.int](http://www.itu.int)

Facebook: [www.itu.int/facebook](http://www.itu.int/facebook)

Twitter: [www.itu.int/twitter](http://www.itu.int/twitter)

## **О партнерстве ИМПАКТ**

Международное многостороннее партнерство против кибербезопасности (ИМПАКТ) является исполнительным органом в области кибербезопасности Международного союза электросвязи – специализированного учреждения ООН по вопросам ИКТ. В качестве первого в мире всестороннего альянса против киберугроз, поддерживаемого ООН, ИМПАКТ объединяет правительства, академические организации и экспертов отрасли в целях повышения способности глобального сообщества решать проблемы, связанные с киберугрозами. Партнерство ИМПАКТ, штаб-квартира которого расположена в Киберджая, Малайзия, является оперативной базой для реализации Глобальной программы кибербезопасности (ГПК) МСЭ. ИМПАКТ обеспечивает 193 Государствам-Членам доступ к специальным знаниям, средствам и ресурсам для эффективного устранения киберугроз, а также оказывает учреждениям Организации Объединенных Наций помощь в защите своих инфраструктур ИКТ.

[www.impact-alliance.org](http://www.impact-alliance.org)