



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

БЮРО РАЗВИТИЯ
ЭЛЕКТРОСВЯЗИ

Документ 014-R
13 декабря 2007 года
Оригинал: английский

6-е СОБРАНИЕ "ВСЕМИРНЫЕ ПОКАЗАТЕЛИ В ОБЛАСТИ ЭЛЕКТРОСВЯЗИ/ИКТ", ЖЕНЕВА, 13–15 ДЕКАБРЯ 2007 г.

ИСТОЧНИК: МСЭ/БРЭ

НАЗВАНИЕ: Оценка готовности к обеспечению национальной кибербезопасности

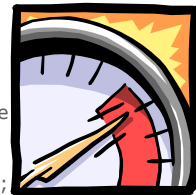
Оценка готовности к обеспечению национальной кибербезопасности

Собрание "Всемирные показатели в
области электросвязи/ИКТ",
Женева, Швейцария
13–15 декабря 2007 года

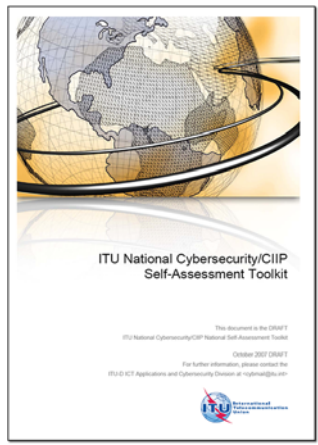
Роберт Шоу
<robert.shaw@itu.int>
Начальник отдела приложений ИКТ и кибербезопасности
www.itu.int/ITU-D/cyb
Департамент политики и стратегии
Сектор развития электросвязи МСЭ (МСЭ-D)

Определение современной ситуации

- В XXI веке увеличивается зависимость от информационно-коммуникационных технологий (ИКТ), охватывающих весь мир;
- Быстрый рост ИКТ и зависимости от них привел к изменению в понимании угроз кибербезопасности в середине 1990-х годов;
- Растет взаимосвязка вопросов кибербезопасности и защиты важнейшей информационной инфраструктуры (СИИП);
- Однако большинство стран не разработали или не реализовали национальные стратегии в области кибербезопасности или программы защиты важнейшей информационной инфраструктуры (СИИП);
- Однако большинство стран не разработали или не реализовали национальные стратегии в области кибербезопасности или программы защиты важнейшей информационной инфраструктуры (СИИП);
- Растет информированность о потребностях, которые должны рассматриваться в рамках национальной политики
 - Но как оценить положение, в котором находятся страны?



Обзор соответствующих видов деятельности Сектора развития МСЭ (МСЭ-D)



- В рамках Вопроса 22/1 Исследовательской комиссии Сектора развития МСЭ представлен Отчет о **передовом опыте** по достижению кибербезопасности
- **Принципы деятельности** в области национальной кибербезопасности/защиты критической инфраструктуры (СИИР)
- **Набор средств для самостоятельной оценки** состояния национальной кибербезопасности/СИИР МСЭ

Декабрь 2007 г.

3

Принципы деятельности в области национальной кибербезопасности/защиты критической инфраструктур

Национальная стратегия	Сотрудничество между правительством и частным сектором отрасли	Сдерживание киберпреступности	Средства контроля происшествий	Культура кибербезопасности
------------------------	--	-------------------------------	--------------------------------	----------------------------

Политика	Политика для руководства действиями на национальном уровне			
Цели	Цели для реализации политики			
Шаги	Шаги для достижений целей			
Ресурсы	Ресурсы в помощь осуществлению действий на национальном уровне			

Конкретные инициативы МСЭ

- МСЭ обеспечивает принципы и поддерживает деятельность по реализации на национальном уровне при помощи
 - ресурсов в виде справочных материалов и профессиональной подготовки
 - <http://www.itu.int/ITU-D/cyb/cybersecurity>
 - набора средств МСЭ для самостоятельного определения состояния национальной кибербезопасности/СИП
 - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
 - региональных мероприятий по принципам кибербезопасности и СИП
 - <http://www.itu.int/ITU-D/cyb/events/>

Региональные мероприятия МСЭ по принципам кибербезопасности/СИП

- 2007 г.
 - Ханой, Вьетнам
 - Буэнос-Айрес, Аргентина
 - Прая, Кабо-Верде
- 2008 г.
 - Оман/Катар
 - Индонезия
 - Латиноамериканские страны
 - Болгария
 - Африка

Современные знания

- Ряд стран выразил заинтересованность в создании индекса готовности к обеспечению национальной кибербезопасности
 - Средство повышения политической информированности о необходимости разработки национальной политики
 - Предоставление сравнительных показателей для оценки положения в стране с выполнением национальных принципов
 - В каком состоянии находится данный процесс?

Сложные задачи, стоящие перед экспертами по показателям

- Как создать индекс, опираясь на элементы **принципов**?
- Некоторые элементы чрезвычайно трудно оценить:
 - национальную стратегию
 - сотрудничество между правительством и частным сектором отрасли
 - сдерживание киберпреступности
 - национальные средства контроля происшествий
 - культуру кибербезопасности

Каковы соответствующие виды деятельности для данного индекса?

- Исследовательский проект ОЭСР по оценке доверия в онлайн-среде
 - > <http://www.oecd.org/dataoecd/26/15/35792806.pdf>
- Виды деятельности Корейского агентства по информационной безопасности
 - > Разработка индекса национальной информационной безопасности
- Соответствие национального законодательства содержательным и процедурным статьям Будапештской конвенции о киберпреступности (2001 год)
- Работа Группы CERT CSIRT над системой показателей для средств контроля происшествий
 - > <http://www.cert.org/csirts/metrics.html>
- Форум по требуемым для признания условиям Групп реагирования на происшествия и безопасности (FIRST) CSIRT?
- Европейское агентство по вопросам сетевой и информационной безопасности (ENISA)
 - > Сбор данных по происшествиям, связанным с безопасностью, и доверию со стороны потребителей, по адресу: http://www.enisa.europa.eu/pages/data_collection/

Международный союз электросвязи

Помогая миру общаться