



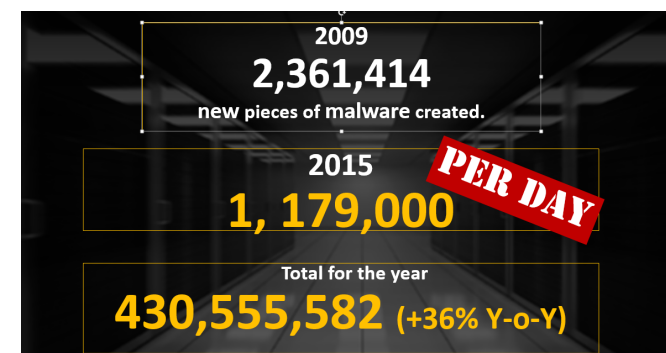
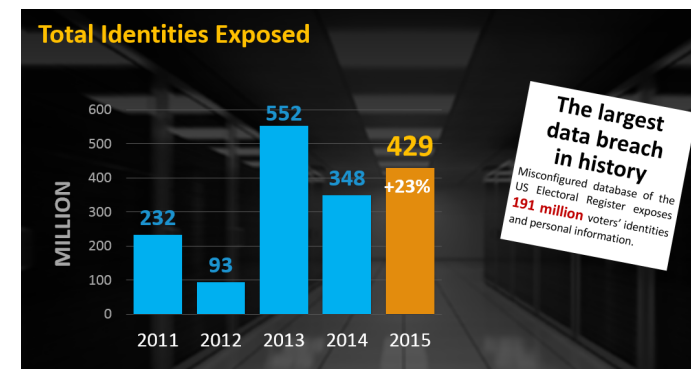
Деятельность МСЭ-D в области кибербезопасности

Фарид Нахли

Координатор программ Зонального отделения МСЭ

Важность кибербезопасности

- От индустриальной эпохи к информационному обществу
 - Растущая зависимость от доступности ИКТ
 - Постоянно растущее количество пользователей сети Интернет (уже 40% населения мира)
- Статистика и отчеты говорят о растущем количестве киберугроз
- Развивающиеся страны более подвержены риску, вследствие быстрого и широкого внедрения ИКТ
- Необходимо создавать человеческий потенциал в сфере кибербезопасности
 - Защита крайне важна для социально-экономического благополучия страны при внедрении новых технологий



2016 Internet Security Threat Report Volume 21

Обзор киберугроз за 2015

- **430 миллионов** новых уникальных **вредоносных программ**
- **9 значимых утечек** (>10 млн идентификаторов) в 2015
- **~191 миллион** идентификаторов раскрыты в рамках **крупнейшей** утечки в истории
- **55% увеличение** количества **фишинговых** кампаний
- **3 из 4** вебсайтов содержат как минимум одну **уязвимость**
- **Половина** всех целевых атак была направлена на предприятия среднего и малого бизнеса

Координированный ответ

На вызовы связанные с кибербезопасностью необходимо дать многоуровневый ответ





Деятельность МСЭ

МСЭ и кибербезопасность

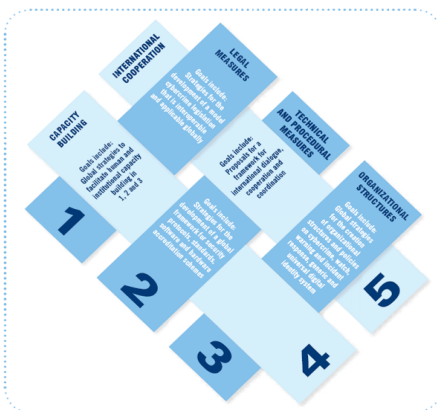


world summit
on the information society
Geneva 2003 - Tunis 2005



2003 – 2005

ВВУИО определили МСЭ как единственного координатора по направлению действия С5 ВВУИО «Доверие и безопасность при использовании ИКТ»



2007

Генеральный Секретарь МСЭ запустил Глобальную повестку кибербезопасности (GCA) – механизм международного сотрудничества по данному вопросу

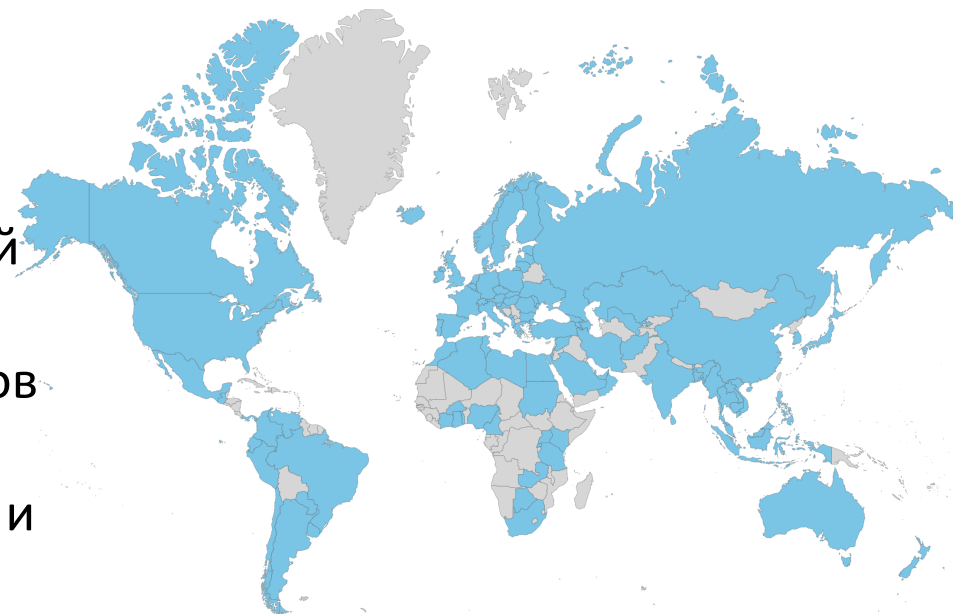


2008 - 2010

Члены МСЭ одобрили GCA в качестве основного инструмента МСЭ по кибербезопасности

Национальные CIRT находятся на передовой борьбы с киберпреступностью

- Реакция на киберпреступления
- Распространение своевременных предупреждений
- Коммуникация и обмен информацией между всеми заинтересованными
- Разработка стратегий снижения рисков и координация мер по реагированию
- Обмен информацией по инцидентам и мерам реагирования
- Публикация лучших практик реагирования и предотвращения угроз
- Координация международного сотрудничества по кибербезопасности



102 национальных CIRT по
всему миру



Программа МСЭ по национальным CIRT

NATIONAL CIRT | CAPACITY BUILDING



- Оценка выполнена для 67 стран
- Реализация выполнена в 11 странах
- Выполняется реализация для 4 стран
- 16 региональных киберисследований (cyber drills) выполнено, суммарно участвовали 115 стран



Цель

Глобальный индекс кибербезопасности (GCI) позволяет оценить насколько серьезно каждая страна относится к вопросу кибербезопасности:

- Законодательная база
- Техническая реализация
- Организационные мероприятия
- Создание потенциала
- Национальное и международное сотрудничество

Задачи

- Продвижение национальных стратегий по кибербезопасности
- Объединение усилий между разными отраслями и секторами
- Интеграция вопросов безопасности в технологический прогресс
- Укрепление глобальной культуры кибербезопасности

Итоговые результаты за 2014 год доступны на сайте МСЭ

Новая версия в 2017 – получено более 127 ответов

<http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx>

Страновые характеристики кибербезопасности

Актуальная информация об уровне кибербезопасности по странам на базе GCA:

- Актуальные документы
- Приглашаем страны содействовать в поддержке актуальности информации

<http://www.itu.int/en/ITU-D/Cybersecurity/Pages/CountryProfiles.aspx>

Пример →



CYBERWELLNESS PROFILE TUNISIA



BACKGROUND
Total Population: 10 705 000 (data source: [United Nations Statistics Division](#), December 2012) Internet users, percentage of population: 43.80% (data source: [ITU Statistics](#), 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION
Specific legislation on cybercrime has been enacted through the following instrument:
[-Art. 199 bis and 199ter](#) of Tunisia Penal Law.

1.1.2 REGULATION AND COMPLIANCE
Tunisia has officially recognized regulations regarding cybersecurity and compliance requirements through the following instruments:
[- Law n° 2004-5](#), February 3, 2004, relative to computer security.
[- Decree n° 1248 - 2004](#), May 25, 2004, setting the administrative, financial and operating procedures of the ANSI.
[- Decree n° 1249 - 2004](#), May 25, 2004, on requirements and procedures for the certification of expert auditors in the field of computer security.
[- Decree n° 1250 - 2004](#), May 25, 2004, on the institutional computer systems and networks subjected to the compulsory periodic Risk Assessment of computer security, and on the criteria relating to the nature and periodicity of the Risk Assessment and to procedures for monitoring the implementation of the recommendations made in the Risk Assessment report.

1.2 TECHNICAL MEASURES

1.2.1 CIRT
Tunisia has an officially recognized National CIRT ([TunCERT](#)).

1.2.2 STANDARDS
There is no information available concerning any officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.



МСЭ взаимодействует с 15 партнерами по разработке и внедрению стратегий кибербезопасности



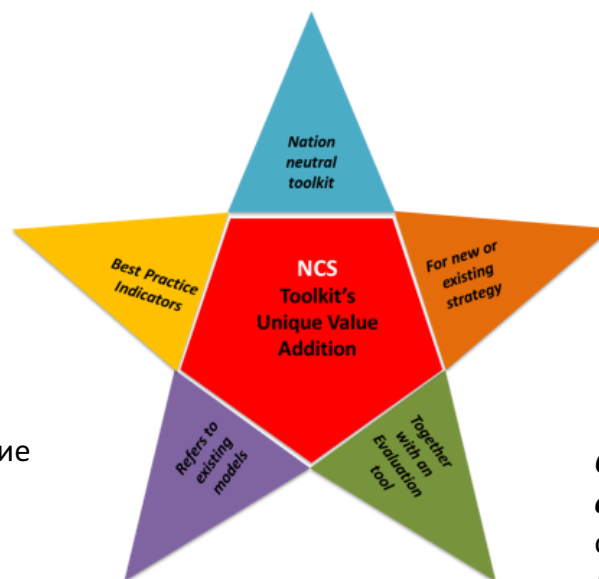
Все партнеры вносят вклад своими знаниями и экспертизой в области кибербезопасности, улучшая качество итоговых материалов

- Разработка инструментов, руководящих указаний, принципов, контрольных списков...
- Реализация национальных стратегий по кибербезопасности
- Финансирование разработки/реализации национальных стратегий по кибербезопасности

Тулкит по разработке национальных стратегий кибербезопасности

Нейтральный тулкит, который может быть применен в любом регионе

Улучшенные измерения:
подбор индикаторов для
оценки прогресса



Практичное руководство, которое может быть использовано странами
для разработки стратегий

Ссылки на другие документы: существующие модели и способы оценки

Сопутствующий механизм оценки: позволяет выявить сферы, требующие улучшения и определить способы улучшения



Первый семинар партнеров в феврале 2016 в Женеве

Второй семинар партнеров в Оксфорде в июне 2016



Построение глобального партнерства

GFCE Основатель и инициатор инициативы CSIRT Maturity

Лучшие практики законодательства, совместная техническая помощь странам, обмен информацией



Symantec **TREND MICRO** Экспертиза глобальных компаний и содействие обмену информацией внутри МСЭ

Сотрудничество в рамках ИТ и киберисследований



Создание потенциала, совместные консультации

Обмен лучшими практиками реагирования на инциденты, совместные мероприятия, содействие в создании CIRT



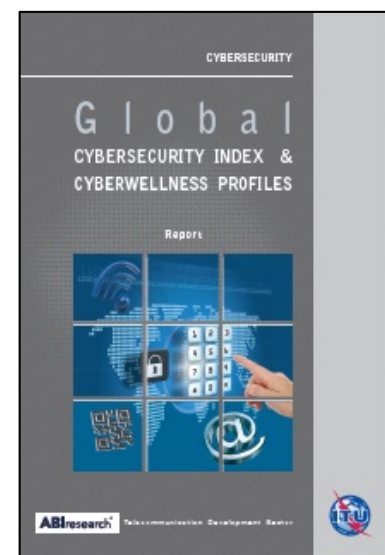
Совместные усилия по борьбе со спамом



8 июня 2015 : Соглашение о создании потенциала в регионе ECOWAS



Публикации



Бесплатная загрузка

<http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx>



Предстоящие мероприятия в регионе

- Региональный семинар МСЭ «Ключевые аспекты кибербезопасности в контексте Internet of Everything (IoE)» (Ташкент, Узбекистан, 19-21 сентября 2017 года)
- Региональные учения по кибербезопасности (Кишинев, Молдова, 7-9 ноября 2017 года)



www.itu.int/cybersecurity

**Спасибо за
внимание
cybersecurity@itu.int**