Развитие культуры кибербезопасности – основные принципы

Андрей Романов
АНО Координационный центр национального домена сети Интернет

Резолюции ООН

Формирование культуры кибербезопасности в соответствии с

резолюциями Генеральной Ассамблеи ООН:

- Резолюция 57/239. Создание глобальной культуры кибербезопасности, 31 января 2003

- Резолюция 58/199. Создание глобальной культуры кибербезопасности и защиты важнейших информационных инфраструктур, 30 января 2004

Резолюция 57/239. Создание глобальной культуры кибербезопасности

Резолюция определяет девять элементов создания глобальной культуры кибербезопасности:

- Повышение осведомленности
- Ответственность
- Реагирование на инциденты
- Этические принципы
- Демократические принципы
- Оценка рисков
- Разработка и реализация мер безопасности
- Управление безопасностью
- Переоценка

Основные проекты в области кибербезопасности (1)

Международные и региональные усилия включают в себя:

- Инициативы Генеральной Ассамблеи ООН (ГА ООН)
- Деятельность в рамках G8
- Конвенцию о киберпреступности Совет Европы
- Инициативы ENISA
- Деятельности Европейской Комиссии
- Деятельности в рамках Регионального содружества в области связи (РСС)
- Инициатвы Шанхайской Организации Сотрудничества
- Организации Азиатско-Тихоокеанского экономического сотрудничества (АТЭС)
- Организация американских государств (ОАГ)

Основные проекты в области кибербезопасности (2)

- Инициативы Лиги арабских государств
- Инициативы Совет сотрудничества стран Залива (GCC)
- Деятельность Организация экономического сотрудничества и развития (ОЭСР)
- Всемирный саммит по информационному обществу (WSIS) и его направление деятельности C5 посвященное укреплению доверия и безопасности при использовании ИКТ
- Проект МСЭ: Глобальная программа кибербезопасности (ГПК)
- МСЭ-D Исследовательская группа 22/1: Рекомендации по развитию культуры кибербезопасности

Роль частного сектора и профильной индустрии

Как владельцы и операторы большинства ИКТ и критической

инфраструктуры, компании частного сектора должны:

- - Играть центральную роль в области кибербезопасности;
- - Использование технической экспертизы частного сектора и его участие имеют первостепенное значение в разработке и реализации национальных стратегий кибербезопасности;
- - Возможности раннего предупреждения и быстрого реагирования имеют ключевое значение для защиты бизнес-активов, во многих странах компании частного сектора, как правило первыми сталкиваются с технологическими изменениями и новыми угрозами;
- Участие бизнеса является ключевым в формировании культуры безопасности посредством разработки стандартов организаций, участия в соответствующих технических форумах безопасности.

Роль частных лиц, гражданского общества и академических кругов

Обеспечение кибербезопасности по сути является общей

ответственностью:

- Правительства и бизнес должны помогать людям получать информацию о том, как защитить себя и, следовательно, общества в целом
- Каждый участник в информационного общества несет ответственность за то, что он предупрежден и может защитить себя, используя правильные и легко доступные инструменты

Основные факторы повышения культуры кибербезопасности (в некоторых странах)

Основные факторы, способствующие развитию культуры

безопасности на национальном уровне:

- - Внедрение приложений и услуг электронного правительства, продвижение электронного бизнеса и коммерческих интернет-приложений;
- - Защита национальных критических, информационных инфраструктур (CII);
- - Защита конфиденциальной информации, как косвенное фактор развития культуры безопасности.

Источник: OECD 2005 Обзор практических инициатив по формированию культуры безопасности

Общие подходы в области кибербезопасности.

При разработке и осуществлении национальной политики в

области культуры кибербезопасности, правительства обычно

используют:

- Междисциплинарный и многосторонний подход;
- Структуры управления высокого уровня;
- Международное сотрудничество в целях формирования культуры безопасности;
- Для обеспечения кибербезопасности важно, чтобы страны были вовлечены в международные связях и сотрудничество в различных областях.

Источник: OECD 2005 Обзор практических инициатив по формированию культуры безопасности

Основные направления деятельности в странах ОЭСР.

Области повышенного внимания:

- Борьба с киберпреступностью;
- Создание национальной группы CERT / CSIRTs (Computer Emergency Response Teams/Computer Security Incident Response Teams);
- Проведение мероприятий по повышению осведомленности в области кибербезопасности;
- Содействие образованию.

Направления с недостаточным вниманием:

- Работа с малыми и средними предприятиями
- Исследование и разработка;
- Анализ и оценка состояния

Источник: OECD 2005 Обзор практических инициатив по формированию культуры безопасности

Роль образования и профессиональной подготовки

При организации национальных усилий кибербезопасности

важно развивать образовательные проекты и учебные

программы для разных категорий участников:

- - Правительствоенных систем и сетей
- - Бизнеса и научных организаций
- - Индивидуальных пользователей и гражданского общества

Необходимо поддерживать инвестиции в области науки и

технологий, а также исследования и разработки.

Независимо от того, какие шаги отдельные страны предпринимают для защиты своих важнейших информационных инфраструктур и для развития культуры кибербезопасности,

никто не будет в безопасности, пока наименее защищенные не будут уделять внимание вопросу кибербезопасноти.

Новые технологии создают не только новые общие возможности, но и общие уязвимости и формируют общую ответственность