Памятные записки по МСЭ

МСЭ: УКРЕПЛЕНИЕ ДОВЕРИЯ К ИКТ И КИБЕРПРОСТРАНСТВУ

Глобальная программа кибербезопасности (ГПК) способствует работе МСЭ по созданию технологических возможностей, необходимых для помощи странам в борьбе с киберугрозами, рекомендует глобальные стандарты в области кибербезопасности и технологии, а также действует в качестве платформы для обмена знаниями и обсуждения вопросов политики.

По прогнозам МСЭ, к концу 2014 года интернетом будут пользоваться почти 3 млрд. человек, что открывает замечательные новые возможности для доступа к информации и связи. Но в то же самое время проблемы с безопасностью и уязвимостью сетей и услуг повсюду приводят к тому, что пользователи подвергаются все более изощренным киберугрозам. Хищение персональных данных, спам, вредоносные программные средства, эксплуатация детей и причинение вреда детям и другим группам, находящимся в особо уязвимом положении, могут иметь драматические и иногда разрушительные последствия для реального мира, не говоря уже о ежегодных потерях для глобальной экономики, которые, по оценкам, составляют 400 млрд. долл. США[1].

Поскольку информационно-коммуникационные технологии (ИКТ) стали важнейшей национальной инфраструктурой, сбой в них может означать катастрофическую приостановку основных услуг. А в среде широкополосных технологий, которые доступны всегда, в любое время, в любом месте, атаки могут быть совершены в какой-либо одной стране, или даже одновременно в нескольких странах, но при этом нарушитель может находиться абсолютно в другом месте.

Кибератаки стали одним из рисков для любой страны, даже наиболее передовой в техническом отношении. Способствовать уменьшению этого риска может более широкое международное сотрудничество.

РАСТУЩАЯ МЕЖДУНАРОДНАЯ УГРОЗА

- В 2013 году насчитывалось почти 400 млн. жертв киберугроз.
- В 2013 году отмечено увеличение на 91% целенаправленных кампаний с целью атак. Количество нарушений возросло на 62%, а 38% пользователей подвижной связи стали жертвами киберпреступности в сетях подвижной связи.
- Количество случаев "вскрытых персональных данных" резко возросло в 2013 году более чем в пять раз до 552 млн. случаев, по сравнению с 93 млн. в 2012 году.
- Тремя секторами, которые наиболее подвержены риску целенаправленных атак, являются государственное управление, добыча полезных ископаемых и обрабатывающая промышленность (Symantec, 2014 Internet Security Threat Report (Отчет об угрозах безопасности в интернете, 2014 г.)).

Пользователи подвижной связи часто хранят файлы с чувствительными данными в онлайновой форме (52%), хранят рабочую и личную информацию в одних и тех же онлайновых учетных записях (24%) и нередко хранят свои имена пользователя и пароли у родственников (21%) и у друзей (18%), что подвергает риску их данные и данные их работодателей. Согласно данным партнера МСЭ компании Symantec, только лишь 50% пользователей принимают самые элементарные меры безопасности.

1. MacAfee

С более подробной информацией о видах деятельности МСЭ можно ознакомиться в блоге МСЭ по адресу: http://itu4u.wordpress.com/.

Инициатива МСЭ "Защита ребенка в онлайновой среде" (COP) представляет собой международную совместную сеть для принятия мер, предназначенных для выявления существующих в мире рисков и уязвимостей для детей в киберпространстве, расширения осведомленности, обмена ресурсами и разработки практических инструментов для оказания помощи в минимизации рисков, а также для содействия формированию ответственного цифрового гражданства.

По мере того как "интернет вещей" становится реальностью, когда миллионы подключенных устройств обмениваются информацией на межмашинном уровне без необходимости вмешательства человека, наш материальный мир и кибермир все более пересекаются. Собирая вместе различные заинтересованные стороны в рамках глобального партнерства, МСЭ находится в авангарде деятельности по обеспечению как технических, так и политических решений вопросов борьбы с киберпреступностью.

Одним из важнейших событий стало создание Глобальной программы кибербезопасности (ГПК) МСЭ – международных рамок для сотрудничества. ГПК способствует работе МСЭ по созданию технологических возможностей, необходимых для помощи странам в борьбе с киберугрозами, рекомендует глобальные стандарты в области кибербезопасности и технологии, а также действует в качестве платформы для обмена знаниями и обсуждения вопросов политики.

Реагирование на национальные кибератаки

Кибератака на национальном уровне может нанести серьезный ущерб важнейшей инфраструктуре, оказывая непосредственное воздействие на повседневную жизнь, начиная от невозможности получить доступ к своим банковским счетам до нарушения работы транспортных сетей, отключения электроэнергии, блокирования связи и еще худших последствий.

Существует явная необходимость в эффективных институциональных структурах по борьбе с инцидентами в киберпространстве и с кибератаками. МСЭ работает вместе с Государствами-Членами, регионами и партнерами по отрасли в целях расширения возможностей по созданию потенциала на национальном и региональном уровнях.

МСЭ способствует созданию потенциала и квалифицированных кадров с помощью обширных программ в области профессиональной подготовки и оказания помощи. Такие инициативы включают:

- Оказание содействия 50 Государствам-Членам в оценке их национальной готовности в области кибербезопасности и потенциала по реагированию. Семи странам была оказана поддержка в создании национальной группы реагирования на компьютерные инциденты (CIRT), а еще семь стран подтвердили, что получают помощь МСЭ.
- На настоящее время проведено семь тренировочных занятий по кибербезопасности для CIRT, в которых участвовали более 60 стран. В ходе этих занятий оценивалось, соответствуют ли основные функции созданных CIRT международным стандартам и передовой практике.
- Разработка национальных стратегий в области кибербезопасности представляет особую проблему для развивающихся стран, у которых нет необходимой нормативно-правовой базы, а также не хватает людского потенциала/квалифицированных кадров и финансовых ресурсов для определения киберугроз, управления ими и реагирования на них. В рамках проекта МСЭ "Повышение кибербезопасности в наименее развитых странах" НРС оказывается содействие в укреплении их потенциала в области кибербезопасности для обеспечения лучшей защиты их национальной инфраструктуры и максимального увеличения социально-экономических преимуществ.
- На региональном уровне дальнейшая помощь предоставляется в форме региональных центров кибербезопасности МСЭ – физического центра,

расположенного на территории того или иного Государства-Члена, который затем выступает в качестве регионального координатора МСЭ по вопросам кибербезопасности. Арабский региональный центр кибербезопасности расположен в Омане, и в настоящее время разрабатываются планы по размещению Африканского регионального центра кибербезопасности в Нигерии.

Безопасность – это основополагающий принцип рекомендаций и стандартов МСЭ, и сейчас все исследовательские комиссии МСЭ регулярно рассматривают связанные с безопасностью вопросы в рамках своей работы.

- МСЭ содействует Государствам-Членам в осмыслении ими правовых аспектов кибербезопасности, с тем чтобы помочь им согласовать свои нормативно-правовые базы, сделав их применимыми на международном уровне и функционально совместимыми.
- Растущая роль ИКТ в предоставлении услуг в столь разнообразных сферах как здравоохранение, образование, финансы и коммерция, означает, что увеличивается необходимость в полностью безопасной киберсреде, несмотря на хроническую повсеместную нехватку квалифицированных специалистов в области кибербезопасности. Чтобы помочь в преодолении такого пробела, МСЭ организовал в различных странах мира учебные семинары-практикумы по кибербезопасности для более 1900 государственных служащих, сотрудников регуляторных органов, а также для специалистов в области ИКТ из государственного и частного секторов.

Защита ребенка в онлайновой среде (COP)

Дети являются одной из самых уязвимых групп в онлайновой среде, при этом новое поколение "цифровых аборигенов" с гораздо большей вероятностью будет раскрывать свои личные данные в сети, что делает их легкими мишенями для преступников и хакеров.

Разделение между онлайновым и реальным миром становится все более расплывчатым, что имеет серьезные последствия для детского психического и физического благополучия. В ходе недавнего исследования почти половина подростков в возрасте от 13 до 17 лет сообщили, что за последний год они подвергались киберзапугиванию в той или иной форме. Еще более настораживает, что три четверти молодых людей, подвергшихся агрессивным сексуальным домогательствам в реальном мире, повстречались со своими агрессорами в онлайновой среде.

Инициатива МСЭ "Защита ребенка в онлайновой среде" (COP) представляет собой международную совместную сеть для принятия мер, предназначенных для выявления существующих в мире рисков и уязвимостей для детей в киберпространстве, расширения осведомленности, обмена ресурсами и разработки практических инструментов для оказания помощи в минимизации рисков, а также для содействия формированию ответственного цифрового гражданства. В рамках COP над достижением этих целей совместно работают более 54 международных партнеров из правительств, частного сектора, гражданского общества, академических организаций и международных организаций.

Технические стандарты (Рекомендации)

Технические стандарты МСЭ (известные как Рекомендации) играют одну из ведущих ролей в деле защиты пользователей в онлайновом пространстве. 17-я Исследовательская комиссия МСЭ-Т является ведущей исследовательской комиссией в области безопасности электросвязи и управления определением идентичности, при этом основное внимание уделяется укреплению доверия и безопасности при использовании ИКТ.

Безопасность – это основополагающий принцип рекомендаций и стандартов МСЭ, и сейчас все исследовательские комиссии МСЭ регулярно рассматривают связанные с безопасностью вопросы в рамках своей работы. К числу достижений на настоящее время относятся: технические Рекомендации для сетей, работающих на основе протокола Интернет (IP), стандарты для сетей последующих поколений (СПП), а также обеспечение четких принципов безопасности для сегодняшних и завтрашних сетей подвижной сотовой связи. Одним из известных примеров является Рекомендация **X.509** – Рекомендация МСЭ-Т по инфраструктуре открытых ключей (PKI) и инфраструктуре управления привилегиями (PMI). В Рекомендации X.509 приводятся, среди прочего, стандартные форматы для сертификатов открытых ключей, списки аннулирования сертификатов и атрибуты сертификатов.

Глобальный подход с участием многих заинтересованных сторон

- Растущая зависимость от ИКТ в наименее развитых странах (НРС) приводит к тому, что кибербезопасность становится все более важным приоритетом, при этом исследования показывают, что развивающиеся страны являются в наибольшей степени уязвимыми, когда речь заходит о киберпреступлениях и киберугрозах. Проект МСЭ "Повышение кибербезопасности в НРС" направлен на защиту пользователей и на то, чтобы сделать интернет более безопасным благодаря обеспечению помощи на уровне политики.
- МСЭ установил партнерские отношения с компанией ABI Research в сфере разработки глобального индекса кибербезопасности (GCI) для обеспечения контрольных показателей национальных возможностей в области кибербезопасности и для того, чтобы Государства-Члены могли учиться на основе передового опыта.
- МСЭ также установил отношения официального сотрудничества с компаниями в области кибербезопасности, такими как Symantec и Trend Micro, с тем чтобы на регулярной основе обмениваться информацией о существующих и появляющихся глобальных тенденциях, относящихся к киберугрозам.
- В настоящее время МСЭ работает вместе с другими учреждениями/организациями системы ООН над укреплением международной координации между учреждениями ООН при оказании ими помощи Государствам-Членам в области кибербезопасности.