Международный союз электросвязи

ВОПРОС 22/1

Заключительный отчет

МСЭ-D 1-я ИССЛЕДОВАТЕЛЬСКАЯ КОМИССИЯ 4-й ИССЛЕДОВАТЕЛЬСКИЙ ПЕРИОД (2006–2010 годы)

ВОПРОС 22/1:

Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности

ИССЛЕДОВАТЕЛЬСКИЕ КОМИССИИ МСЭ-D

В соответствии с Резолюцией 2 (Доха, 2006 г.) ВКРЭ-06 сохранила две исследовательские комиссии и определила Вопросы для исследования в них. Рабочие процедуры, которые должны применяться в этих исследовательских комиссиях, описаны в Резолюции 1 (Доха, 2006 г.), принятой на ВКРЭ-06. На период 2006–2010 годов 1-й Исследовательской комиссии было поручено исследование девяти Вопросов в сфере "Стратегия и политика в области развития электросвязи". 2-й Исследовательской комиссии было поручено исследование девяти Вопросов в сфере "Развитие служб и сетей электросвязи и приложений ИКТ и управление ими".

За более подробной информацией

Просьба обращаться к:

Mr Souheil MARINE/Ms Christine SUND
Бюро развития электросвязи (BDT)
ITU
Place des Nations
CH-1211 GENEVA 20
Switzerland
Тел.: +41 22 730 5323/ 5203
Факс: +41 22 730 5484
Эл. почта: souheil.marine@itu.int
christine.sund@itu.int

Размещение заказов на публикации МСЭ

Просим принять к сведению, что заказы не могут приниматься по телефону. Их следует направлять по факсу или по электронной почте.

ITU
Sales Service
Place des Nations
CH-1211 GENEVA 20
Switzerland
Факс: **+41 22 730 5194**
Эл. почта: **sales@itu.int**

Электронный книжный магазин МСЭ: www.itu.int/publications

ВОПРОС 22/1

Заключительный отчет

МСЭ-D 1-я Исследовательская комиссия 4-й Исследовательский период (2006–2010 гг.)

ВОПРОС 22/1:

Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности

ЗАЯВЛЕНИЕ ОБ ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТИ

Настоящий отчет подготовлен многочисленными добровольцами из различных администраций и организаций. Упоминание конкретных компаний или видов продукции не является одобрением или рекомендацией МСЭ. Выраженные мнения принадлежат авторам и ни в коей мере не влекут обязательств со стороны МСЭ.

СОДЕРЖАНИЕ

Стр.

ВОПРОС 22-1

Введение

В настоящем отчете вниманию национальных администраций предлагается обзор структурных элементов, необходимых для решения проблем кибербезопасности на национальном уровне и выработки подхода к обеспечению национальной кибербезопасности[1]. Поскольку существующие национальные возможности меняются, а угрозы непрерывно совершенствуются, в настоящем отчете не предлагается готовых рецептов обеспечения безопасности в киберпространстве. Вместо этого он содержит описание гибких подходов, которые можно применить, для того чтобы помочь национальным администрациям проанализировать и усовершенствовать существующие институты, политику и взаимоотношения в сфере кибербезопасности. Хотя основное внимание в данном отчете уделяется вопросам кибербезопасности, мы отмечаем, что защита физической сети имеет такое же приоритетное значение. Мы отмечаем также, что передовой опыт в области обеспечения кибербезопасности должен защищать и уважать конфиденциальность и свободу волеизъявления, которые содержатся в соответствующих частях Общей декларации по правам человека и Женевской декларации принципов построения информационного общества[2].

Ключевыми элементами отчета являются:

- разработка национальной стратегии в области кибербезопасности;
- установление сотрудничества на национальном уровне между государственными органами и частным сектором;
- предотвращение киберпреступлений;
- создание национального потенциала для управления инцидентами; и
- содействие развитию национальной культуры кибербезопасности.

Каждый из этих элементов должен являться частью общего национального подхода к вопросам кибербезопасности. Порядок их перечисления не дает предпочтения одному элементу перед другим. Он может быть другим, в зависимости от национальных условий.

Для целей настоящего отчета термин ***кибербезопасность*** определяется Рекомендацией X.1205 МСЭ-Т как набор средств, стратегий, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологий, которые могут быть использованы для защиты киберпространства, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность имеет своей целью обеспечение и поддержание параметров безопасности ресурсов организации и пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее:

- доступность;
- целостность, которая может включать аутентичность и сохранность информации;
- конфиденциальность.

Важно понимать взаимосвязь между кибербезопасностью, важнейшей инфраструктурой (CI), важнейшей информационной инфраструктурой (CII), защитой важнейшей информационной

---

[1] Заинтересованным читателям предлагается обратиться к выходной информации стандартов ИСО 27001–27003.

[2] См. ВВУИО, Тунисская программа для информационного общества, пункт 42.

инфраструктуры (CIIP) и инфраструктурой, не относящейся к важнейшей. Эта взаимосвязь представлена на Рисунке 1.

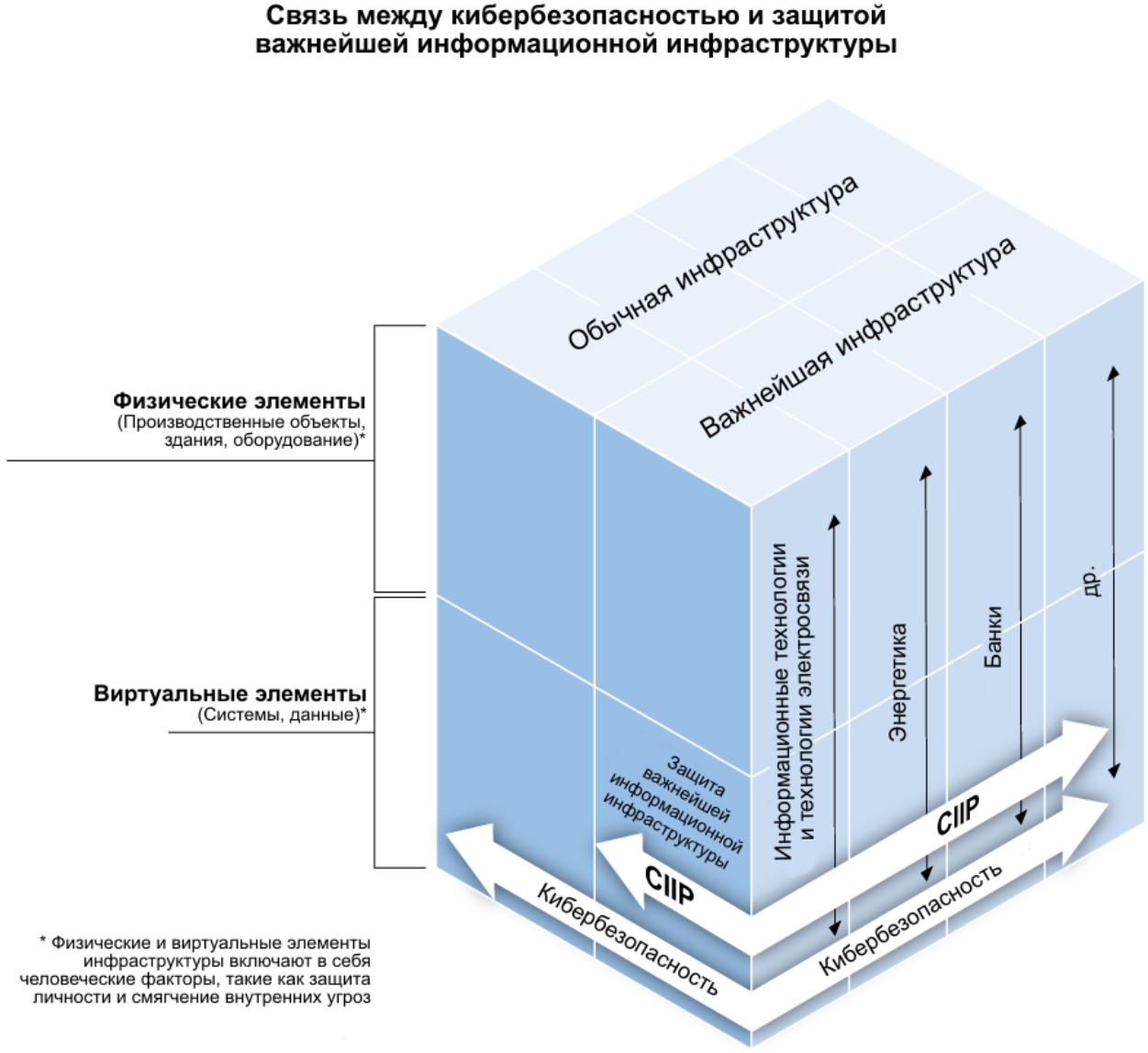
Хотя определения могут незначительно отличаться, ***важнейшими инфраструктурами*** (CI), как правило, считаются ключевые системы, услуги и функции, неисправность или разрушение которых оказывает пагубное влияние на систему общественного здравоохранения и безопасности, коммерческую деятельность и национальную безопасность или на их сочетание. CI состоят как из материальных (например, зданий и сооружений), так и виртуальных элементов (например, систем и данных) (см. Рисунок 1). Каждая страна может иметь свое понимание термина "важнейший", однако обычно это понятие может включать в себя элементы информационно-коммуникационных технологий (ИКТ) (включая электросвязь), энергетику, банковское дело, транспорт, общественное здравоохранение, сельское хозяйство и продовольствие, водоснабжение, химическую промышленность, судоходство, а также важнейшие государственные службы. На всех этапах своего развития странам необходимо планировать и разрабатывать стратегии по защите того, что они считают CI (другими словами, защита информационной инфраструктуры, включающей и физическую, и виртуальную защиту) для того, чтобы обеспечить разумные гарантии устойчивости и безопасности от внешних воздействий для выполнения общегосударственных задач и поддержания экономической стабильности.

Каждый из этих секторов экономики имеет свои собственные материальные ресурсы, например здания банков, электростанции, поезда, больницы и правительственные офисы. Вместе с тем все эти важнейшие секторы национальной экономики зависят от информационно-коммуникационных технологий. Эти секторы и их материальные ресурсы без всяких исключений зависят от надежного функционирования этой ***важнейшей информационной инфраструктуры*** (CII), позволяющей им предоставлять свои услуги и вести хозяйственную деятельность. Поэтому серьезный сбой в CII может иметь незамедлительные и пагубные последствия, далеко выходящие за пределы сектора ИКТ и оказывающие влияние на способность государства выполнять свои важнейшие задачи во многих секторах. Программа ***защиты важнейшей информационной инфраструктуры*** (CIIP) защищает виртуальный компонент CII.

Как показано на Рисунке 1, CIIP является подгруппой и CIP, и кибербезопасности. Кибербезопасность защищает от всех видов инцидентов в киберпространстве, повышая безопасность важнейшей информационной инфраструктуры, от которой зависят важнейшие сектора, а также обеспечивая защиту сетей и служб, которые служат удовлетворению повседневных потребностей пользователей. Инциденты в киберпространстве могут одинаковым образом затрагивать важнейшие инфраструктуры и инфраструктуры, не являющиеся важнейшими, и могут проявляться в виде разнообразных действий злоумышленников, таких как использование сетевых роботов для совершения атак типа "отказ в обслуживании" и распространение спама и вредоносных программ (например, вирусов или "червей"), влияющих на возможность работы сетей. Кроме того, инциденты в киберпространстве могут включать в себя незаконные виды деятельности, например "фишинг" и "фарминг", а также хищение персональных данных. Киберугрозы продолжают нарастать, поскольку используемые инструменты и методики становятся все более доступными, технические возможности киберпреступников расширяются, а их действия становятся все более изощренными. С инцидентами в киберпространстве сталкиваются страны, находящиеся на любых стадиях развития.

Национальный подход к вопросам кибербезопасности включает в себя повышение осведомленности относительно существования рисков в киберпространстве, создание национальных структур, занимающихся вопросами кибербезопасности, и установление необходимых взаимоотношений, которые могут быть использованы для ликвидации возникающих инцидентов. Оценка риска, применение мер по смягчению последствий, и устранение последствий также являются составной частью национальной программы по обеспечению кибербезопасности. Эффективная программа по обеспечению кибербезопасности поможет защитить экономику страны от сбоев, способствуя планированию непрерывности бизнеса в различных секторах, защищая информацию, хранящуюся в информационных системах, сохраняя общественное доверие, поддерживая национальную безопасность и обеспечивая общественное здравоохранение и безопасность.

Рисунок 1: Концептуальная взаимосвязь между защитой важнейшей информационной инфраструктуры и кибербезопасностью



Повышение кибербезопасности не может ограничиваться только национальной стратегией, хотя она и очень важна. Оно должно дополняться региональными и международными стратегиями, которые предусмотрены соответствующими решениями ВВУИО на двух этапах ее работы в 2003–2005 годах и последующей деятельностью по направлению С5, основанными на пунктах 35 и 36 Женевской декларации принципов и пункте 39 Тунисской программы, а также выполнением решений Всемирной встречи на высшем уровне по вопросам информационного общества, которые отражены в соответствующих Резолюциях, мерах и инициативах, принятых МСЭ, например:

a) Цель 4 Резолюции 71 (Пересм. Анталия 2006 г.) ПК "Стратегический план Союза на 2008–2011 годы".

b) Резолюция 130 (Пересм. Анталия 2006 г.) ПК "Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий".

c) Соответствующие части Дохинского плана действий, принятого на ВКРЭ-06, включая Программу 3 по электронным стратегиям и ИКТ приложениям, которые определяют кибербезопасность как приоритет для БРЭ с принятием определенных действий и в особенности принятием Резолюции 45 (Доха, 2006 г.) "Механизмы совершенствования сотрудничества в области кибербезопасности, включая борьбу со спамом". Резолюция 45 поручает Директору БРЭ организовывать собрания для обсуждения путей усиления кибербезопасности, включающих среди прочего, меморандум взаимопонимания, с целью усиления кибербезопасности и борьбы со спамом в заинтересованных Государствах – Членах Союза и сообщить о результатах этих собраний на Полномочной конференции 2006 года. Доклад БРЭ к ПК 2006 года находится по адресу: http://www.itu.int/md/S06-PP-C-0024/en[3].

d) Большая работа ведущей 17-й Исследовательской комиссии МСЭ-Т по кибербезопасности и дополнительные действия 13-й Исследовательской комиссии.

e) Последняя Резолюция 58, принятая на ВАСЭ (Йоханнесбург, 2008 г.) "Стимулирование создания национальных групп реагирования на компьютерные инциденты (CIRT), в частности для развивающихся стран", которая признала работу, проводимую Сектором МСЭ-D по Вопросу 22/1.

f) В отчете председателя Группы экспертов высокого уровня (HLEG) по Глобальной программе кибербезопасности (ГПК), начатой Генеральным секретарем 17 мая 2007 года, содержится резюме предложений экспертов по семи основным стратегическим целям, входящим в эту инициативу, с акцентом на соответствующие Рекомендации для следующих пяти стратегических принципов:

- правовые меры;
- технические и процедурные меры;
- организационная структура;
- создание потенциала;
- международное сотрудничество.

Среди данных областей работы, "правовые меры" сосредоточены на вопросе о том, как решать законодательные проблемы, связанные с преступлениями, совершаемыми в ИКТ сетях в масштабе, совместимом с международным. "Технические и процедурные меры" сосредоточены на ключевых мерах, предназначенных для ускорения принятия расширенных подходов для усиления безопасности и управления рисками в киберпространстве, включающих схемы аккредитации, протоколы и стандарты. "Организационные структуры" сосредоточены на предотвращении, обнаружении, реагировании и управлении рисками кибератак, включая защиту систем важнейшей информационной инфраструктуры. "Создание потенциала" сосредоточено на разработке стратегий для механизмов укрепления потенциала, с целью повышения информированности, обмена ноу-хау и повышения кибербезопасности в программе национальной политики. Наконец, "Международное сотрудничество" сосредоточено на международном сотрудничестве, диалоге и координации в борьбе с киберугрозами[4, 5].

g) Последний проект Мнения 4, принятого Всемирным форумом по политике в области электросвязи (ВФПЭ) 2009 года, о "Совместных стратегиях по укреплению доверия

---

[3] Арабские государства, исходя из своего опыта последних четырех лет, больше убеждены в том, что наиболее эффективным способом удовлетворения глобальных и/или региональных потребностей Государств-Членов в отношении усиления кибербезопасности и борьбы со спамом является МоВ.

[4] Эксперты из арабских государств поддержали все рекомендации, содержащиеся в отчете председателя HLEG.

[5] С подробной информацией об отчете председателя HLEG можно ознакомиться по адресу: http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf.

и безопасности при использовании ИКТ"[6], отмечающий, в частности, разделы *предлагает МСЭ* и *предлагает Государствам-Членам*.

h) Деятельность БРЭ в соответствии с Программой 3 (электронные приложения) в виде прямой помощи развивающимся Государствам – Членам Союза, посредством разработки проектов и наращивания потенциала/набора средств МСЭ для самостоятельной оценки состояния национальной кибербезопасности/CIIP, набора средств МСЭ для защиты от бот-сетей и инструментария для создания национальных CIRT.

i) Инициатива "Защита ребенка в онлайновой среде" (COP) была выдвинута в ноябре 2008 года в виде международной совместной сети для принятия мер по содействию защите детей и молодежи во всем мире путем предоставления руководящих указании по безопасному поведению в онлайновой среде во взаимодействии с другими учреждениями и партнерами ООН. Основными целями инициативы COP являются: 1) выявление существующих в киберпространстве основных рисков и уязвимостей для детей и молодежи; 2) формирование осведомленности относительно рисков и проблем, используя для этого разные каналы; 3) разработка практических инструментов в помощь правительствам, организациям и преподавательскому составу при проведении деятельности по снижению в возможной степени рисков; и 4) обмен знаниями и опытом на основе содействия международному стратегическому партнерству по определению и реализации конкретных инициатив.

j) Сотрудничество, налаженное между МСЭ и Международным многосторонним партнерством против киберугроз (ИМПАКТ) в рамках Глобальной программы кибербезопасности (ГПК), направлено на то, чтобы свести вместе представителей основных заинтересованных сторон и партнеров из государственных органов, компаний частного сектора и от научного мира, в целях обеспечения Государств – Членов МСЭ специальными знаниями, средствами и ресурсами для эффективного устранения кибеугроз. Основными целями сотрудничества между МСЭ и ИМПАКТ являются: 1) разработка глобальной основы для наблюдения за инцидентами, предупреждения о них и реагирования в случае их возникновения; 2) создание надлежащих национальных и региональных институциональных структур и стратегий, таких как группы реагирования на компьютерные инциденты (CIRT); 3) содействие созданию институционального и человеческого потенциала во всех секторах; и 4) содействие развитию глобального международного сотрудничества между многими заинтересованными сторонами.

---

[6] С полным текстом проекта Мнения 4 ВФПЭ можно ознакомиться по адресу: http://www.itu.int/osg/csd/wtpf/wtpf2009/documents/opinion4.pdf.

ЧАСТЬ I

Разработка и достижение соглашения в отношении национальной стратегии кибербезопасности

Разработка и реализация национального плана в области кибербезопасности требует наличия всеобъемлющей стратегии, включающей предварительный всесторонний анализ пригодности существующей национальной политики и анализ роли в этом процессе всех заинтересованных сторон (правительственных органов, частного сектора и граждан).

Исходя из соображений обеспечения национальной безопасности и экономического благосостояния, правительства должны создать возможности для защиты своих важнейших информационных инфраструктур, стимулировать и обеспечивать эту защиту. В настоящее время информационные инфраструктуры проникают во все секторы промышленности государств и пересекают национальные границы. Повсеместный характер важнейших информационных инфраструктур открывает широчайшие возможности и дает огромные экономические преимущества.

Эти преимущества также влекут за собой дорогостоящие взаимозависимости и риски. В исследовании, проведенном по заказу Бюро развития электросвязи (БРЭ) МСЭ, эти затраты представляются следующим образом[7]:

> Вредоносные программы и спам оказывают влияние на затраты и доходы всех заинтересованных сторон в сети коммерческого предоставления информационных услуг, таких как производители программного обеспечения, операторы сетей, поставщики услуг интернета (ПУИ) и пользователи. Это влияние включает в себя, в том числе, затраты на превентивные меры, затраты на ликвидацию последствий, прямые затраты на пропускную способность и на оборудование, а также возможные затраты, связанные с перегрузкой сети. Ситуация еще больше осложняется тем фактом, что спам и вредоносные программы создают также новые потоки доходов как законного, так и незаконного характера. Они обеспечивают возможность существования законных бизнес-моделей (например, антивирусные и антиспамовые продукты, инфраструктура и полоса пропускания), а также преступных бизнес-моделей (сдача внаем сетевых роботов, комиссионные от продаж, обусловленных спамом, фондовые схемы "накачки и сброса" и др.). Следовательно, они создают смешанные, иногда противоречивые стимулы для заинтересованных сторон, которые усложняют принятие согласованных решений для этой проблемы.

На протяжении многих лет большинство стран считают национальную коммутируемую телефонную сеть общего пользования (КТСОП) важнейшей инфраструктурой и обеспечивают ей соответствующую защиту. Во многих странах коммерческие компании владеют значительной частью инфраструктуры КТСОП, сотрудничая в этой деятельности с правительством и друг с другом. Вместе с тем, стремительное развитие цифровых ИКТ в условиях взаимных соединений проводных и беспроводных сетей связи резко изменило природу безопасности сетей и предъявляемые к ней требования и, возможно, привело к тому, что многие традиционные направления политики и процедуры в отношении безопасности на КТСОП оказываются недостаточными для удовлетворения новых требований в отношении такой безопасности.

В результате производимых ИКТ изменений необходимо уделять существенно больше внимания сотрудничеству органов государственного управления, коммерческих структур, других организаций и отдельных пользователей, которые разрабатывают информационные системы и сети, владеют ими, предоставляет услуги, управляют ими, осуществляют их обслуживание и используют их. Хотя за органами государственного управления зачастую сохраняется ведущая роль в разработке государственной политики в отношении безопасности сетей, необходимо добиться того, чтобы и другие заинтересованные стороны, в том числе операторы и разработчики инфраструктуры, участвовали в

---

[7] См. проект исследования "Финансовые аспекты безопасности сетей: вредоносные программы и спам", МСЭ-D 1/144 (6 мая 2008 г.).

общем процессе планирования и разработки политики. Работая вместе, правительство и частный сектор могут эффективно использовать свои специальные знания и управлять рисками для CII. Такая интеграция способствует укреплению доверия и обеспечивает наиболее эффективную разработку и применение политики и технологий. На международном уровне защита важнейших информационных инфраструктур и укрепление кибербезопасности требуют установления сотрудничества и координации действий между государствами, а также с международными партнерами.

I.A Обзор целей, относящихся к настоящей части

I.A.1 Добиться на уровне национальной политики понимания проблем кибербезопасности и необходимости действий на национальном уровне и международного сотрудничества.

I.A.2 Разработать национальную стратегию по усилению кибербезопасности в целях уменьшения рисков и последствий от кибернетических и физических сбоев.

I.A.3 Участвовать в международных действиях, направленных на поддержание национальных действий по предотвращению инцидентов, обеспечению готовности к ним, реагированию на них и восстановлению после них.

I.B Конкретные меры для достижения этих целей

Вышеупомянутые цели являются общими для всех стран; вместе с тем конкретные меры, принимаемые для реализации этих целей, будут различаться в зависимости от потребностей каждой страны и обстановки в ней. Во многих странах эти меры будут принимать национальные органы государственного управления.

I.B.1 Убедить руководителей государства и правительство в необходимости принятия на национальном уровне мер по борьбе с угрозами и устранению уязвимости национальной киберинфраструктуры в рамках обсуждения на политическом уровне.

1 Для страны, намеревающейся усилить кибербезопасность и обеспечить безопасность своей важнейшей информационной инфраструктуры, первым шагом является придание кибербезопасности статуса национальной политики. Программное заявление страны, касающееся кибербезопасности, как правило, 1) признает важность CII для страны; 2) определяет риски, с которыми она сталкивается (обычно используется подход, учитывающий все риски[8]); 3) определяет цель политики в области кибербезопасности; и 4) в общих чертах определяет пути ее реализации, включая сотрудничество с соответствующими структурами.

После того как общая политика в области кибербезопасности четко определена, она может быть более подробно сформулирована в национальной стратегии, в которой распределяются роли и сферы ответственности, определяются приоритеты, устанавливаются временные рамки и показатели ее реализации. Кроме того, политика и стратегия могут включать национальные усилия в контекст других видов международной деятельности в области кибербезопасности. Для реализации общей политики в области кибербезопасности, возможно, потребуется повысить осведомленность ключевых фигур, принимающих решения, относительно этих проблем. Лица, принимающие решения, должны понимать, что для достижения согласованных целей кибербезопасности может потребоваться длительный период времени.

2 Национальная структура кибербезопасности не должна состоять из незыблемых стратегий. Напротив, эта структура и стратегии должны быть гибкими и реагировать на динамичную среду рисков. Эта структура должна определять цели политики. Установив четкие цели

---

[8] Подход ко всем факторам риска или многофакторный подход к управлению рисками включает рассмотрение всех потенциальных естественных и технологических опасностей, т. е. включает естественные и искусственные (случайные или намеренные) чрезвычайные ситуации и бедствия.

политики, правительственные учреждения и неправительственные организации могут наиболее эффективно сотрудничать в достижении заявленных целей.

3 Такую национальную политику следует разрабатывать совместно, консультируясь с представителями всех заинтересованных групп участников, включая правительственные учреждения, частный сектор, научное сообщество и соответствующие ассоциации. Эта политика должна быть провозглашена на национальном уровне, предпочтительно главой правительства.

I.B.2 Определить ключевую фигуру и ведущее учреждение для деятельности на национальном уровне в целом; решить, в какой из государственных структур следует создать группу реагирования на инциденты, связанные с компьютерной безопасностью[9], с полномочиями общенационального уровня[10], а также определить ведущие учреждения по каждому аспекту национальной стратегии.

1 Для начала реализации инициативы по обеспечению кибербезопасности необходимо определить, кто на первоначальном этапе возглавит национальную деятельность в сфере кибербезопасности, – это должен быть государственный служащий политического уровня, который понимал бы проблемы кибербезопасности и мог бы направлять и координировать действия государственных учреждений и эффективно взаимодействовать с частным сектором. В идеале это лицо должно обладать политическим авторитетом и иметь доступ к главе правительства. Положение столь высокого уровня необходимо для того, чтобы обеспечить координацию структур, которые должны взаимодействовать друг с другом. Постепенно эти усилия по координации позволят сформировать институциональный фундамент для технических лидеров страны в сфере кибербезопасности и соответствующих организаций.

2 После того как страна выступила с инициативой по обеспечению кибербезопасности, лицу или учреждению, предпринявшему эти усилия, возможно больше не потребуется играть такую роль.

3 Следует определить, какие другие учреждения будут отвечать за разработку и реализацию различных частей национальной стратегии безопасности.

I.B.3 Определить соответствующих экспертов и разрабатывающих политику лиц в органах государственной власти и частном секторе, а также установить их функции.

1 Для принятия эффективных мер на национальном уровне необходимо привить всем участникам "культуру кибербезопасности". Все лица и учреждения, относящиеся и не относящиеся к органам государственного управления, которые занимаются разработкой информационных систем и сетей, владеют или управляют ими, обслуживают и используют их, должны понимать свои функции и действия, которые они должны осуществить. Служащие высшего звена, занимающиеся разработкой политики, и руководители частного сектора должны установить в своих учреждениях цели и приоритеты. Технические служащие высшего звена должны обеспечить руководящие принципы и основу для действий.

I.B.4 Определить формы сотрудничества между всеми участниками и для них.

---

[9] CSIRT представляет собой Группу экспертов по безопасности ИТ, главной деятельностью которой является реагирование на инциденты в области компьютерной безопасности. Она предоставляет необходимые услуги, с тем чтобы управлять ими и помогать своим избирателям исправлять нарушения ("Подход шаг за шагом, о том как создать CSIRT" находится по адресу: http://www.enisa.europa.eu/act/cert). Группы CSIRT также иногда называют Группой компьютерной "скорой помощи" или Группой быстрого реагирования на компьютерные инциденты (CERT), CSIRTS и CERTS выполняют те же функции. Термин "компьютер" в аббревиатуре CSIRT в том числе используется в настоящем докладе, с тем чтобы охватить, например, маршрутизаторы, серверы, подвижные IP-устройства и связанные с ними приложения.

[10] В данном отчете национально определяемый CSIRT будет называться "CIRT".

1 Национальные органы государственного управления должны содействовать разработке механизмов официального и неофициального сотрудничества, которые способствовали бы контактам частного сектора и органов государственного управления и совместному использованию ими информации. На техническом или оперативном уровнях кибербезопасность будет внедряться широким кругом как правительственных, так и неправительственных учреждений. Эту деятельность также следует координировать и предусмотреть для нее механизмы совместного использования информации.

I.B.5 Создать механизмы сотрудничества между структурами государственного управления и частного сектора на национальном уровне.

1 Разработка политики и составление, и выполнение национального плана должны осуществляться в рамках открытых и прозрачных процессов. При этом следует принимать во внимание взгляды и интересы всех участников.

I.B.6 Определить международных партнеров и содействовать международным усилиям, направленным на решение проблем кибербезопасности, включая совместное использование информации и оказание помощи, с учетом результатов проекта по осуществлению Резолюции 45 ВКРЭ-06.

1 Деятельности по повышению уровня национальной кибербезопасности будет способствовать участие в региональных и международных форумах, где может обеспечиваться обучение и профессиональная подготовка, зачастую в форме конференций и семинаров-практикумов. Такие форумы повышают осведомленность по соответствующим проблемам, дают возможность ознакомиться с докладами специалистов и позволяют странам обмениваться идеями, опытом и перспективами. Этому может способствовать участие и/или членство в региональных и международных организациях, стремящихся к достижению тех же целей. Это является одной из целей проекта по осуществлению Резолюции 45.

2 Участие в существующих программах и видах деятельности в рамках многосторонних организаций, стремящихся улучшить и повысить глобальную кибербезопасность, является еще одним способом содействия развитию международного сотрудничества. Примеры многосторонних организаций включают Международный союз электросвязи (Направление деятельности С5 ВВУИО), Организацию экономического сотрудничества и развития (ОЭСР), Организацию американских государств (ОАГ) и Азиатско-Тихоокеанскую ассоциацию экономического сотрудничества (АТЭС) и др. Кроме того, имеются и другие конференции, в рамках которых правительства могут обмениваться информацией по вопросам кибербезопасности, такие как Меридианная конференция.

3 Кроме того, следует учитывать также возможность участия в деятельности, организуемой частным сектором, например в работе Рабочей группы против "фишинга" и аналогичных международных усилиях.

I.B.7 Наладить интегрированный процесс управления рисками в целях определения защитных мер и их приоритетности в отношении кибербезопасности.

1 Только осознав риски, правительственные органы, владельцы инфраструктур и операторы (включая поддерживающих их поставщиков) могут приступить к налаживанию сотрудничества частного бизнеса государства и граждан в целях определения ключевых функций и элементов защиты и установления в отношении них приоритетов. После того как определены функции важнейшей информационной инфраструктуры, они могут быть распределены в порядке приоритетности или классифицированы по степени их важности в зависимости от конкретных условий. Важно помнить, что понятие "важности" зависит от конкретной ситуации, и поэтому то, что может быть важным в одном случае, в другом случае может оказаться не столь важным. Поскольку страны сами определяют важнейшие функции и устанавливают в отношении них приоритеты, то они должны помнить, что критерий важности будет изменяться по мере совершенствования технологий, инфраструктур и процессов.

2 Обеспечение защиты CII и киберпространства является весьма сложным делом. Защита CII, киберпространства и важнейших функций, которые они выполняют, предполагает постоянное применение целого ряда практических методов управления рисками (т. е. проведение оценки угрозы, уязвимости и последствий, определение мер по обеспечению безопасности и смягчению последствий, внедрение мер по обеспечению безопасности и оценка их эффективности), позволяющих операторам управлять рисками и обеспечивать устойчивость при выполнении основных задач. Поставщики информационных инфраструктур, каждый в отдельности, как правило, имеют в своем распоряжении современные методики и практические методы управления рисками, поскольку они оказывают услуги в режиме реального времени. Вместе с тем наличие присоединений, взаимозависимость и техническая сложность информационной инфраструктуры ограничивают возможность быстро и легко оценивать общий риск или готовность. В результате, использование сотрудничества между государственными органами и частным сектором значительно облегчает оценку рисков, связанных с взаимозависимостью и совместным использованием инфраструктуры (стихийное бедствие, технологический отказ, террористическая атака и т. д.).

I.B.8 Оценить современное состояние деятельности в области кибербезопасности, периодически проводить его переоценку и разработать программные приоритеты.

1 В национальную стратегию кибербезопасности следует включить национальное оценочное обследование, которое можно было бы использовать для самооценки хода работы или в качестве составной части деятельности по профессиональной подготовке или вспомогательной оценке. Используя общий механизм самооценки, страны могли бы выявить сильные стороны и потенциальные разрывы в своей национальной структуре и наметить процесс приведения их в соответствие с желаемыми целями. (Набор средств МСЭ для самостоятельной оценки состояния национальной кибербезопасности/CIIP был разработан БРЭ в дополнение к данному документу, содержащему передовой опыт).

I.B.9 Определить потребности в профессиональной подготовке и способы их удовлетворения.

1 В результате сопоставления рекомендуемого передового опыта, приводимого в настоящем отчете, и фактической практики в сфере кибербезопасности (т. е. проведения сравнительного анализа) та или иная страна может обнаружить, что некоторые аспекты ее программы кибербезопасности нуждаются в совершенствовании. Это может требовать решения в технической сфере (например, применения нового оборудования или программного обеспечения), правовой сфере (например, разработки новых законов или регламентарных норм для борьбы с ненадлежащим поведением в киберпространстве) или организационного решения. Сравнительный анализ также, вероятно, покажет, в каких сферах необходимо дополнительное наращивание человеческого потенциала (профессиональная подготовка).

ЧАСТЬ II

Налаживание сотрудничества между государственными органами и частным сектором

Защита важнейшей информационной инфраструктуры и киберпространства является общей обязанностью, которая может быть наилучшим образом реализована посредством сотрудничества между правительственными органами на всех уровнях и частным сектором, владеющим значительной частью инфраструктуры и эксплуатирующим ее. Несомненно, правительства должны иметь решающее слово в любых национальных решениях, которые приняты. Важно признать, что хотя системы информационной безопасности в мире стали в основном полностью совместимыми и взаимосвязанными, структура такой сети в различных странах может быть различной. Поэтому сотрудничество между владельцами и операторами этих систем может способствовать созданию эффективной и устойчивой системы безопасности.

Как правительство, так и частный сектор принципиально заинтересованы в обеспечении устойчивости инфраструктуры. Соответственно, частно-государственное партнерство является основой для усиления кибербезопасности, ибо ни одна организация в одиночку не сможет защитить всю инфраструктуру. Поскольку значительная часть киберинфраструктуры во многих странах находится в собственности и/или эксплуатируется частным сектором, правительственным органам и частному сектору рекомендуется целенаправленно сотрудничать в рамках их соответствующих функций. Для обеспечения эффективного [частно-государственного] сотрудничества требуется наличие трех важных элементов: 1) четкое ценностное предложение; 2) четкое разграничение функций и обязанностей; и 3) доверие.

Ценностное предложение

Успех партнерства зависит от разъяснения партнерам из правительственных органов и частного сектора взаимных выгод. Выгоды для правительственных органов заключаются в том, что поставщики и операторы инфраструктур обладают возможностями, которые обычно выходят за рамки основных полномочий правительственных органов, например:

- владение и управление большей частью основной инфраструктуры во многих секторах и во многих странах;
- знание ресурсов, сетей, систем, средств, функций и других возможностей;
- специальные знания и опыт реагирования на инциденты;
- возможность введения новшеств и предоставления продуктов, услуг и технологий для быстрого удовлетворения соответствующих потребностей; и
- проектирование, развертывание, эксплуатация, управление и обслуживание глобального интернета.

При оценке ценностного предложения для частного сектора становится очевидной выгода от сотрудничества с правительственными органами для усиления CIIP и кибербезопасности. Правительственные органы могут внести свой вклад в совместную деятельность разными способами, которые включают:

- предоставление владельцам и операторам своевременной, аналитической, достоверной, обобщенной и полезной информации об угрозах основной инфраструктуре;
- вовлечение частного сектора с самого начала в разработку инициатив и политики в отношении CIIP;
- разъяснение руководителям корпораций, используя открытые платформы и прямое общение, выгоды, как для коммерческих предприятий, так и для национальной безопасности, инвестирования в меры по обеспечению безопасности, выходящие за рамки их конкретных деловых стратегий;

- создание условий, стимулирующих и поддерживающих инициативы, направленные на то, чтобы компании добровольно внедряли широко распространенные, надежные меры по обеспечению безопасности и, в случае необходимости, обновляли и совершенствовали свою деятельность и практические методы по обеспечению безопасности, выходящие за пределы потребностей, диктуемых их узко местническими деловыми интересами;
- работа с частным сектором в целях формулирования и четкого определения приоритетов в отношении основных функций и обеспечения их защиты и/или восстановления;
- оказание поддержки научно-исследовательской деятельности, необходимой для наращивания будущих усилий по защите CI;
- определение ресурсов для участия в исследованиях о взаимозависимости различных секторов путем проведения научных диспутов, симпозиумов, учебных занятий и компьютерного моделирования, которые позволяют получить информацию для руководства при принятии решений, необходимую для планирования непрерывности бизнеса; и
- обеспечение возможности для обмена срочной информацией, а также для восстановления и поддержки важнейших инфраструктурных сооружений и услуг во время инцидента.

Функции и обязанности

Правительственные органы и частный сектор могут совместно выработать общее понимание своих функций и обязанностей, относящихся к кибербезопасности. Правительственные органы могут обеспечить координацию и руководство усилиями в области защиты. Так, например, непрерывное функционирование механизма государственного управления требует обеспечения безопасности и готовности кибернетической и физической инфраструктуры правительств, необходимых для поддержания ее основных функций и услуг. Кроме того, правительство может играть ключевую координирующую роль в период катастроф или может оказать помощь в случаях, когда частный сектор испытывает нехватку ресурсов, для того чтобы реагировать на инциденты. Правительство может стимулировать и поощрять добровольные усилия частного сектора для повышения безопасности, включая разработку политики и протокола, необходимых для своевременного обмена аналитической и практической информацией об угрозах, и обеспечение стимулов для частного сектора в целях усиления безопасности до уровней, выходящих за пределы потребностей, диктуемых их корпоративными интересами. И наконец, правительство может оказать поддержку и профинансировать проведение научных исследований и разработок в целях совершенствования процессов и инструментария.

Доверие

Важнейшим элементом успешного сотрудничества между правительственными органами и частным сектором является доверие. Доверие необходимо для установления, развития и поддержания взаимных связей между правительственными органами и частным сектором. Прочное сотрудничество и обмен информацией между частным сектором и правительством позволяют лучше ориентироваться в обстановке, облегчают сотрудничество по стратегическим вопросам, помогают управлять рисками в киберпространстве и способствуют осуществлению деятельности по реагированию и восстановлению. Путем эффективного обмена информацией и ее анализа и правительство, и частный сектор будут лучше подготовлены к выявлению угроз и наиболее уязвимых мест, а также к тому, чтобы обмениваться тактическими приемами и ресурсами, направленными на смягчение и предотвращение последствий.

Ниже приводится перечень общих целей, которые должны учитываться правительственными органами по мере того, как они сотрудничают с частным сектором.

II.A Обзор целей, относящихся к настоящей части

II.A.1 Разработать механизм сотрудничества, основанного на частно-государственных взаимоотношениях, направленный на эффективное управление рисками в киберпространстве и защиту киберпространства.

II.A.2 Обеспечить механизм для сведения воедино различных концепций, активов и знаний для достижения консенсуса и совместного продвижения вперед в целях усиления безопасности на национальном уровне.

II.B Конкретные меры для достижения этих целей

II.B.1 Учитывать перспективы частного сектора на ранних стадиях разработки и реализации политики в области безопасности и связанной с ней деятельности.

1 Во многих странах основные инфраструктуры, а также кибернетические компоненты, на которые они опираются, находятся в частной собственности или эксплуатируются частными предприятиями. Технологии, формирующие и поддерживающие киберпространство, быстро развиваются, используя инновации частного сектора. Поэтому правительственные органы в одиночку не могут обеспечить эффективную защиту киберпространства. Осведомленность о перспективах развития частного сектора и включение в процесс главных владельцев и операторов основной инфраструктуры имеет неоценимое значение для деятельности правительства в области кибербезопасности, связанной с разработкой и реализацией стратегии кибербезопасности, а также созданием условий для управления рисками. Правительственные органы могут получать информацию от частного сектора путем участия в деятельности рабочих групп, включающих представителей правительственных органов и частного сектора, запросов о предоставлении комментариев частного сектора при разработке политики и стратегии в отношении кибербезопасности, а также путем координации усилий с организациями частного сектора с использованием механизмов обмена информацией. Правительственные органы должны обеспечить участие частного сектора в разработке, реализации и поддержании инициатив и стратегии на начальных этапах этого процесса.

2 Правительственные органы и частный сектор должны совместно внедрять подход к управлению рисками, позволяющий правительственным органам и частному сектору определять киберинфраструктуру, анализировать угрозы, оценивать уязвимость, возможные последствия и определять средства для их смягчения.

3 Правительственные органы и частный сектор должны совместно заниматься исследованиями и разработками (R&D), направленными на обеспечение управления рисками. Понимание приоритетов в отношении R&D, а также инициативы, предпринимаемые правительственными органами и частным сектором, могут способствовать выделению и эффективному использованию ресурсов, своевременному проведению R&D и, в конечном итоге, своевременной разработке продуктов и услуг в целях усиления национальной кибербезопасности.

II.B.2 Поощрять создание групп частного сектора от различных отраслей основной инфраструктуры для решения проблем безопасности совместно с органами государственного управления.

1 Формирование таких групп, например ассоциаций деловых кругов, в различных секторах основной инфраструктуры поможет решить общие проблемы в сфере кибербезопасности. Эти группы могут заниматься стратегическими и/или оперативными вопросами и решением проблем безопасности, касающихся [частного сектора] в целом. К таким проблемам можно отнести управление рисками, повышение информированности, разработку и осуществление политики, и многие другие вопросы. Эти группы инфраструктуры частного сектора позволяют создать институциональные рамки для взаимодействия с органами государственного управления и могут служить форумом для доверительного диалога по вопросам кибербезопасности.

2 В некоторых странах такие группы были созданы несколькими связанными с важнейшей инфраструктурой секторами, представители которых обмениваются информацией по угрозам, факторам уязвимости и возможным последствиям в сфере безопасности. Зачастую эти группы также обеспечивают своим членам оповещение и предупреждение в режиме

реального времени, что способствует деятельности по смягчению последствий реальных инцидентов, затрагивающих важнейшие инфраструктуры, реагированию на них и восстановлению после них.

3 Эти группы должны подумать о внедрении практических методов, позволяющих осуществлять сотрудничество и обмениваться информацией между членами (т. е. правительственными органами и частным сектором) в рамках пользующихся доверием форумов. Некоторые из этих методов могут включать обеспечение следующего: анонимности для членов; доступа к информации различных секторов и правительственной информации; доступа к продуктам, восприимчивым к угрозам и уязвимости, а также к аналитическим продуктам; заключений специалистов по конкретным вопросам, касающимся координации деятельности по реагированию в чрезвычайных условиях, практики эксплуатации и опытных мероприятий. При рассмотрении этих практических методов для обеспечения возможностей сотрудничества, важно включить меры защиты прав собственности и чувствительной с точки зрения коммерции информации.

II.B.3 Организовать общение групп частного сектора и органов государственного управления в рамках пользующихся доверием форумов для решения общих проблем в сфере безопасности.

1 Для обеспечения доверия и содействия развитию эффективного сотрудничества между органами государственного управления и частным сектором необходимо соблюдение ряда условий. Рекомендуется письменное соглашение относительно сотрудничества и обмена между органами государственного управления и частным сектором. Участникам необходимы общая концепция и цель. Сильное индивидуальное или коллективное руководство должно определять приоритеты, распределять ресурсы и устанавливать обязательства, необходимые для поддержания частно-государственного сотрудничества. Для определения индивидуальных и коллективных норм поведения в рамках отношений сотрудничества требуются также определенные правила взаимодействия.

2 Участники должны видеть ощутимые и измеримые результаты. Разработка предложений, касающихся выгод и преимуществ сотрудничества для отдельных лиц и организаций и четкое разъяснение ценности такого сотрудничества является ключевым фактором развития и поддержания отношений [частно-государственного] сотрудничества.

II.B.4 Поощрять сотрудничество между группами, относящимися к взаимозависимым отраслям.

1 Инциденты, затрагивающие один тип инфраструктуры, могут оказывать каскадное воздействие и приводить к возникновению инцидентов в инфраструктурах других типов. Так, перебои в электроснабжении могут привести к нарушениям работы интернета и телефонной связи. Наряду с этим, планируя принятие мер в случае чрезвычайных ситуаций в одном секторе, следует учитывать, какое воздействие они могут оказывать на другие секторы. Обмен информацией по различным инфраструктурам поможет осуществлять деятельность по реагированию на инциденты, которые охватывают несколько секторов одновременно и имеют общенациональное значение.

II.B.5 Заключать договоренности о сотрудничестве между органами государственного управления и частным сектором для управления деятельностью при инцидентах.

1 Оперативное обнаружение инцидентов, обмен информацией и принятие мер зачастую способны сократить масштабы ущерба, наносимого киберинцидентами. На национальном уровне [частно-государственное] сотрудничество необходимо для проведения анализа, оповещения и координации мер реагирования.

2 Органам государственного управления и следует совместно разработать основу для координации стратегических и оперативных мер и повышения осведомленности для совершенствования управления деятельностью при инцидентах. Эта основа должна содержать официальный механизм для обмена информацией, включающий координаторов по вопросам политики и обмена оперативной информацией. Эта основа должна также включать политику и процедуры совместного использования, сообщения об инцидентах, защиты и распространения важнейшей конфиденциальной информации (правительственных

органов и частного сектора), а также механизмы передачи и распространения информации. Информация частного сектора зачастую является собственностью компаний, и ее обнародование может привести к потере доли рынка, неблагоприятному освещению деятельности компаний и другим негативным последствиям. Аналогичным образом, информация органов государственного управления может быть закрытой или секретной и не подлежать обнародованию. Следует применять меры политического и технического характера для защиты информации, не ущемляя при этом прав общества на получение информации. Органы государственного управления могут и далее укреплять доверие, совершенствуя политику в отношении обмена информацией и взаимоотношений с частным сектором путем оценки политических мер на постоянной основе. Можно также проводить киберучения для проверки каналов связи между органами государственного управления и частным сектором и координации при реагировании на киберинциденты и восстановлении после них, применяя механизмы, которые используются при реальных кризисных ситуациях.

ЧАСТЬ III

Предотвращение киберпреступности

Кибербезопасность может быть значительно улучшена путем, помимо прочего, разработки и совершенствования поддерживающего ее уголовного законодательства, судопроизводства и политики, направленных на предотвращение, сдерживание киберпреступности, реагирования на нее и преследование в судебном порядке.

III.A Обзор цели, относящейся к настоящей части

III.A.1 Принять всеобъемлющий комплекс законов, относящихся к кибербезопасности и киберпреступности.

Каждой стране необходимы законы, касающиеся киберпреступности как таковой, процедур расследования в электронной форме и оказания помощи другим странам. Эти законы могут относиться к одному разделу кодекса законов или размещаться в разных его разделах. Для простоты в настоящем документе предполагается, что у каждой страны имеется один основной закон по киберпреступности и ряд связанных с ним правовых документов по процессуальным вопросам и оказанию взаимной помощи. Несомненно, страны должны использовать любую структуру, которая, как они полагают, наилучшим образом подходит к их национальным условиям.

III.B Конкретные меры для достижения этой цели

III.B.1 Оценить адекватность существующих правовых руководств. Страна должна проанализировать свой действующий уголовный кодекс, включая существующие процедуры, с тем чтобы определить, пригоден ли он для решения текущих (и будущих) проблем. Рекомендуемые шаги:

1 Разработать, при необходимости, необходимое соответствующее законодательство, учитывающее, в частности, региональные инициативы. Такое законодательство должно регулировать, помимо прочего, вопросы, касающиеся порчи или уничтожения компьютерных данных; процессуальные механизмы, обеспечивающие проведение расследований и включающие возможность выяснения происхождения сообщений электронной почты и т. д.; и включая возможное правовое сотрудничество (например, получение доказательств и т. д.)

2 Странам следует выяснить, не основываются ли их законы на устаревших технических представлениях. Например, закон может предусматривать возможность отслеживания передач только голосовой информации. Возможно, этот закон необходимо изменить, с тем чтобы он охватывал также и передачу данных.

3 Закон о киберпреступности в той или иной стране должны оценить все заинтересованные в нем правительственные и законодательные органы власти, даже в том случае, если они не имеют отношения к уголовному правосудию, чтобы не упустить какую-либо полезную идею. Например, занимающийся информационными технологиями служащий может заметить, что закон о киберпреступности не охватывает новую технологию, которая используется все в более широких масштабах, но еще не получила известность среди разработчиков законов в стране.

4 Кроме того, рекомендуется, чтобы действующее уголовное законодательство стран также прошло оценку со стороны некоторых или всех ниже перечисленных структур: местного частного сектора, какого-либо местного филиала международного частного сектора, местных неправительственных организаций, научных кругов, признанных экспертов или групп граждан.

5 Любая страна может обратиться за советом по таким вопросам к другим странам.

III.B.2 Разработать и принять законы и направления политики по материальному праву, процессуальным вопросам и взаимной помощи для борьбы с киберпреступностью.

1 Рекомендовать странам активно участвовать в разработке, при необходимости, необходимого законодательства, учитывающего, в частности, региональные инициативы, включая, помимо прочего, Конвенцию Совета Европы по киберпреступности. Рекомендовать странам принимать участие в региональном и международном сотрудничестве в целях борьбы с киберпреступностью и укрепления кибербезопасности, а также разработать механизмы расширения сотрудничества в области кибербезопасности, включая борьбу со спамом, вредоносными программами, сетевыми роботами и т. д.

2 Все правительственные и законодательные органы власти должны оценить проект национального закона о киберпреступности. Этот проект должен быть также общедоступен для замечаний, с целью учета всех возможных технологий, нарушений или других соответствующих вопросов, которые первоначально не были охвачены.

3 Любой закон по киберпреступности должен относиться не только к классическим киберпреступлениям, таким как компьютерные преступления и компьютерное вмешательство, но также защищать электронное доказательство в сетях относительно других преступлений.

4 Законы о защите данных, действующие в отношении гражданской жизни и экономики, не следует распространять или интерпретировать таким образом, чтобы ненадлежащим образом препятствовать передаче доказательств по уголовным делам из одной страны в другую.

5 Странам, привлекающим консультантов для разработки проекта закона, следует изучить их квалификацию и установить постоянный контроль за их работой. Лица, не прошедшие соответствующую подготовку по законодательству конкретной страны, могут оказаться не в состоянии адекватно отразить все необходимые положения, в особенности в отношении разделов по процессуальным вопросам и взаимной правовой помощи. Наряду с этим маловероятно, что лица, не имеющие опыта работы в прокуратуре, должным образом учтут практические аспекты доказывания версии по делу. Некоторые консультанты имеют надлежащую квалификацию для помощи в составлении законов об электронной торговле, но не уголовных законов.

6 Можно обратиться к другим странам за предложениями, выходящими за рамки конвенции. Например, странам может быть необходимо, чтобы поставщики услуг интернета сохраняли часть проходящих через их системы данных на протяжении некоторого времени, часто на протяжении полугода; или они могут нуждаться в том, чтобы органам власти сообщали о компьютерных инцидентах определенной значимости; или они могут потребовать предоставления надлежащего удостоверения личности для использования интернет-кафе.

7 Если время позволяет, страна может получить замечания по проекту закона о киберпреступности (или поправки к нему) от других стран и многосторонних организаций. Такие замечания можно получить в частном порядке, и, как отмечалось выше, было бы полезно узнать точки зрения нескольких стран, основанные на их опыте.

8 На возможно более ранней стадии (в соответствии с принятыми в стране процедурами) страна может запросить замечания у тех, кто имеет законный интерес в данном вопросе, – местного частного сектора, какого-либо местного филиала международного частного сектора, местных неправительственных организаций, научных кругов, отдельных заинтересованных граждан и других.

III.B.3 Учредить или определить национальные группы по киберпреступности.

1 Важно, чтобы в любой стране, вне зависимости от уровня развития, имелся хотя бы базовый потенциал расследования киберпреступлений. Так, использование сотовых телефонов стремительно распространяется даже в развивающихся странах, а с помощью сотовых телефонов можно совершать мошенничества, переводить деньги, устраивать заговоры, передавать вирусы в электронные сети, производить взрывы и т. д.

2 Каждая страна должна отобрать или подготовить полицейскую службу или службы, которые были бы способны расследовать киберпреступления. Иногда не вызывает сомнений вопрос о том, о какой службе или каких службах должна идти речь. Иногда право заниматься этой работой оспаривают несколько полицейских служб, и верховной власти приходится принимать непростое решение. Даже если окажется, что в стране в настоящее время нет кадров, обладающих необходимыми навыками, обычно где-то служит полицейский, который интересуется электронными технологиями, стремится узнать больше и продвинуться в этой области.

3 Группы по расследованию киберпреступлений, даже если их состав включает только ограниченное количество следователей, нуждаются в поддержке. Им требуется относительно современное оборудование, достаточно надежные сетевые соединения и постоянная профессиональная подготовка. Такая поддержка может оказываться правительством страны, международными организациями или другими странами либо осуществляется на средства частного сектора.

4 Там, где это возможно, желательно, чтобы группы обладали хотя бы базовым компьютерным потенциалом для криминалистической работы. Для создания такого потенциала потребуется программное обеспечение и дополнительная профессиональная подготовка. (Если считается, что судебный потенциал создать невозможно, странам следует заранее признать, что могут быть утрачены имеющие решающее значение данные даже по важнейшим делам.) При определенных обстоятельствах судебная помощь по отдельным случаям может предоставляться другими странами. Наряду с этим профессиональная подготовка по киберкриминалистике может проводиться другими странами и соответствующими организациями. Так, Координационный центр групп реагирования на компьютерные инциденты университета Карнеги-Меллона в Соединенных Штатах (http://www.cert.org/) предлагает курсы по киберкриминалистике бесплатно или по весьма умеренным расценкам в онлайновом режиме или на CD-ROM.

5 После создания группа по киберпреступности должна заявить о своем существовании и потенциале другим полицейским службам страны и прокуратуре. Нет смысла держать группу по киберпреступности в столице, если региональная полиция, расследующая тяжкое преступление, по которому имеются доказательства в электронной форме, не знает, что существует группа по киберпреступности, которая может проверить содержимое компьютера подозреваемого или оказать какую-то иную помощь. К сожалению, повсеместно и довольно часто правоохранительные органы не в курсе того, что в стране есть группа по киберпреступности.

6 Группам по киберпреступности или группам, которым предстоит работать в этой области, следует в максимально возможной степени содействовать развитию связей с международными партнерами. На первоначальных стадиях получить совет о том, как создать такую группу, можно у других стран и международных полицейских организаций. На более поздних стадиях различные виды профессиональной подготовки и даже аппаратное и программное обеспечение можно получить от других стран, международных полицейских организаций, соответствующих многосторонних организаций и частного сектора. Такие контакты важны и еще по одной причине: в мире, который во все большей мере становится сетевым, решающее значение имеет возможность запросить помощь у правоохранительных органов за рубежом.

7 Группам по киберпреступности следует также установить связи со всеми соответствующими и заинтересованными структурами в своих странах, например, с национальными неправительственными организациями, группами реагирования на инциденты в сфере компьютерной безопасности, объединениями частного сектора и научными кругами, с тем чтобы они знали о существовании и возможностях соответствующей группы, могли сотрудничать с ней, а также о том, как сообщать о возможных киберпреступлениях.

III.B.4 Установить отношения сотрудничества с другими звеньями национальной инфраструктуры кибербезопасности и частным сектором.

1 Отношения сотрудничества между органами власти, другими звеньями национальной инфраструктуры кибербезопасности и частным сектором важны по нескольким причинам:

a) для обмена информацией между этими группами (например, чтобы сообщить о подготовке нового закона или разработке новой технологии);

b) для обмена мнениями (например: "Если мы составим новый закон таким образом, не кажется ли вам, что возникнут проблемы с неприкосновенностью частной жизни?" или "Можно ли так видоизменить данную технологию, чтобы на законных основаниях в сфере общественной безопасности все же можно было отслеживать происхождение сообщений электронной почты?");

c) для взаимного предоставления возможностей профессиональной подготовки, хотя обычно именно частный сектор предлагает профессиональную подготовку органам государственного управления;

d) для обмена сведениями о существующих угрозах и факторах уязвимости;

e) чтобы работники различных структур достаточно хорошо познакомились, чтобы доверять друг другу в чрезвычайных ситуациях.

2 При налаживании таких отношений сотрудничества можно предусмотреть в качестве разумного первого шага, чтобы один или несколько человек составили список людей и организаций в стране, обладающих специальными знаниями и функциями в кибернетической области во всех соответствующих секторах. В списке можно будет отразить контактную информацию об этих людях. Вероятно, лучше не придавать списку официального характера, чтобы избежать разногласий относительно того, кого туда вносить, а кого нет.

3 В каждой стране наверняка имеется множество соответствующих структур, которые в состоянии помочь в обеспечении кибербезопасности, – законодатели, министерства, неправительственные организации, группы реагирования на инциденты в сфере компьютерной безопасности, научные круги, объединения частного сектора и отдельные лица. Некоторые из них могут работать только в пределах страны, а другие – быть связанными с более крупными иностранными структурами.

III.B.5 Добиться понимания работниками прокуратуры, судьями и законодателями проблем киберпреступности.

1 Для успешного решения вопросов киберпреступности важно, чтобы работники прокуратуры и судьи разбирались в таких областях, как компьютеры, программное обеспечение и сети, а также понимали растущее значение доказательств в электронной форме. Точно так же и законодатели должны иметь некоторое представление об этих вопросах, а также понимать, пригодны ли законы страны для борьбы с киберпреступностью. Одним из способов решения этой проблемы является профессиональная подготовка.

2 Если требуется базовая техническая подготовка, ее можно получить из различных источников в зависимости от имеющихся в стране ресурсов:

a) от любой имеющейся в стране службы или министерства, компетентных в технических вопросах, например полицейской службы или министерства информационных технологий;

b) от правительств других стран;

c) от соответствующих многонациональных организаций;

d) от местного частного сектора;

e) от международного частного сектора, в особенности (но не исключительно), если он действует на местном уровне;

f) от соответствующих научных кругов;

g) от национальных или иностранных групп реагирования на инциденты в сфере компьютерной безопасности; и

h) от национальных и иностранных соответствующих неправительственных организаций.

3 Может также оказаться полезным провести подготовку руководителей высшего звена, разрабатывающих политику, государственных служащих и т. п. в отношении того, что угрожает электронным сетям (например, каким образом может подвергнуться нападению национальная банковская система) и какую угрозу представляют электронные сети (например, использование интернета для нахождения уязвимых детей и торговли ими в сексуальных целях). Подготовку по этим аспектам электронных сетей обычно можно получить из вышеупомянутых источников.

4 Подготовка может быть желательна для прокуроров и судей относительно судебного преследования киберпреступности или других преступлений, связанных с электронными данными, или методов организации международного сотрудничества. Такую подготовку можно получить у:

a) какой-либо национальной службы или министерства, обладающего соответствующей компетенцией, например прокуратуры или министерства юстиции;

b) правительств других стран;

c) соответствующих многонациональных организаций;

d) соответствующих научных кругов;

e) соответствующих национальных и иностранных неправительственных организаций; и

f) соответствующих частных лиц.

5 Та или иная страна может нуждаться в профессиональной подготовке по вопросам разработки законодательства. Такую подготовку можно получить у структур, перечисленных в пункте выше. Возможными источниками специальных знаний могут быть местный частный сектор и международный частный сектор, в особенности (но не исключительно) если он ведет дела на местном уровне. Однако структуры частного сектора, скорее всего, смогут оказать содействие в отношении законов об электронной торговле, а не в отношении законов о киберпреступности, уголовно-процессуальных норм и международной взаимной правовой помощи.

6 По всем этим видам подготовки обучающие источники могут предложить проводить ее в запрашивающей стране, или же они могут предложить модули для подготовки (в электронной или печатной форме), по которым инструкторы из запрашивающей страны могут сами провести подготовку. В некоторых случаях, например при подготовке CERT-CC, описываемой в разделе III.B.3.4, подготовка может предоставляться бесплатно или за минимальную плату.

7 В некоторых странах ключевым фактором осознания на национальном уровне проблем киберпреступности стала поддержка со стороны служащих высшего звена, иногда даже одного авторитетного руководителя, в особенности в сфере бюджетного контроля. Если известно, что министр весьма интересуется кибербезопасностью, его или ее министерство – а, возможно, и все правительство – будет охотнее поддерживать сотрудников рабочего уровня, которые пытаются чего-то добиться на местах.

III.B.6 Участвовать в сети контактных центров 24/7 по киберпреступности.

1 В 1997 году основные развитые страны, входящие в Подгруппу по преступлениям, с использованием высоких технологий Группы восьми (G8), начали работы с министрами юстиции и министрами внутренних дел стран G8 над вопросами контактной сети по киберпреступности, работающей в режиме 24/7, для того чтобы улучшить международную помощь в срочных исследованиях, касающихся электронных доказательств. Многие следователи, занимавшиеся киберпреступностью, считали, что было слишком сложно узнать, где можно оперативно получить помощь от других стран. Наряду с этим многие следователи считали, что заключенные десятки лет назад договоры о правовой взаимопомощи не пригодны для стремительно меняющейся судебной практики, связанной, например, с полуночными вторжениями в компьютерную сеть финансовой системы той или иной страны. На начало 2008 года созданная сеть охватывает почти 50 стран. Сеть открыта для участия любой страны, обладающей необходимым потенциалом для оказания помощи, о которой говорится ниже.

2 Для присоединения к сети страна должна иметь контактный центр, работающий двадцать четыре часа в сутки семь дней в неделю – отсюда неофициальное название: "сеть 24/7". Контактный центр может представлять собой лицо, с которым можно связаться напрямую или через какое-либо учреждение. Это лицо должно быть компетентно в трех областях: 1) технологии, чтобы запросы можно было направлять, не тратя время на длинные технические пояснения; 2) внутреннего права страны; и 3) в вопросах о том, какие возможности предоставляются ему внутренним правом для оказания помощи другим странам. Если само контактное лицо не обладает знаниями в этих трех областях, оно должно иметь возможность, если потребуется, незамедлительно (а не в следующий приемный день) связаться с любым правомочным лицом в его/ее органах государственного управления, которое уполномочено оказать ему помощь.

3 По меньшей мере, первоначально связь должна осуществляться между контактным центром 24/7 в стране A и контактным центром 24/7 в стране B, с тем чтобы обеспечить последовательность и безопасность. Это означает, что контактные центры не должны сообщать контактную информацию другим учреждениям в своей стране. Напротив, контактные центры должны осуществлять первый международный контакт от имени запрашивающего учреждения (например, полицейского управления провинции) в своей стране. После налаживания первоначального сотрудничества между двумя странами контактный центр, по желанию сторон, может устраниться от расследования и предоставить соответствующему полицейскому управлению провинции страны A возможность непосредственно общаться со страной B.

4 Подключаясь к сети, страны не гарантируют, что всегда будут помогать друг другу, и контактная сеть не заменяет обычной взаимной правовой помощи между странами. Точнее говоря, контактная сеть только гарантирует, что запрашивающей стране будет немедленно, даже ночью, уделено грамотное, компетентное внимание. После оказания первоначальной помощи страны могут предложить (а могут и не предлагать) использовать менее экстренные каналы взаимной помощи.

5 Круглосуточный режим доступности не означает, что в офисе день и ночь функционирует определенное количество автоматизированных рабочих мест и ряд киберследователей готовы отвечать на телефонные звонки и сообщения электронной почты. В большинстве стран такого офиса не существует. Обычно по телефону можно связаться с одним из сотрудников полиции (из дежурной смены), который, возможно спит, имея под рукой сотовый телефон.

6 Для подключения к сети странам следует связаться с председателем Подгруппы по высокотехнологичным преступлениям Группы восьми (ее членство не ограничивается Группой восьми, к сети уже подключились почти 50 стран). Требуется заполнить короткий и

несложный формуляр[11]. Нет необходимости заключать официальные международные соглашения, такие как меморандумы о взаимопонимании и договоры. Периодически сеть 24/7 организует для контактных центров профессиональную подготовку и сетевые конференции. Путевые издержки по этим конференциям субсидируются по мере необходимости.

7 Включенная в сеть группа обязана сообщить местным или национальным полицейским службам и группам по киберпреступности о своем существовании и готовности оказывать помощь в осуществлении контактов за рубежом.

[11] Этот формуляр следует направить по факсу: +202 514 6113 на имя координатора, 24/4 Network, Computer Crime and Intellectual property Section, US Dep of Justice, Washington, D.C., USA. Его можно также направить по эл. почте по адресу: richard.green@usdoj.gov.

ЧАСТЬ IV

Создание национального потенциала по управлению инцидентами: наблюдение, предупреждение, реагирование и восстановление

Для органов государственного управления важно создать или определить национальную организацию, которая являлась бы координирующим органом по обеспечению безопасности киберпространства и защиты важнейшей информационной инфраструктуры, основной задачей которого являлась бы деятельность по наблюдению, предупреждению, реагированию и восстановлению, а также содействие сотрудничеству между правительственными органами, частным сектором, научными кругами и международным сообществом.

Одной из основных функций органов государственного управления при обеспечении кибербезопасности на национальном уровне является обеспечение готовности к киберинцидентам, их обнаружение, реагирование на возникающие инциденты и их устранение. Внедрение механизма по устранению инцидентов требует учета аспектов, касающихся финансирования, наличия людских ресурсов, профессиональной подготовки, технического потенциала, взаимоотношений между органами государственного управления и частным сектором, а также правовых требований. Необходимо сотрудничество на всех уровнях государственного управления, а также сотрудничество с частным сектором, научными кругами и международными организациями в целях согласования имеющихся возможностей и специальных знаний для устранения инцидентов и повышения осведомленности о возможных атаках и способах борьбы с ними. Правительство играет ключевую роль в обеспечении координации деятельности между этими организациями.

IV.A Обзор целей, относящихся к настоящей части

Создание национального потенциала для устранения инцидентов требует осуществления целого ряда тесно связанных видов деятельности, включающих:

IV.A.1 Разработку согласованной общегосударственной системы реагирования в случае нарушения безопасности киберпространства для предотвращения, обнаружения, сдерживания киберинцидентов, реагирования на них и восстановления после таких инцидентов.

IV.A.2 Создание координирующего органа по устранению киберинцидентов, который объединил бы важнейшие элементы правительственных структур (включая органы правопорядка) и основной потенциал операторов и поставщиков инфраструктур, для того чтобы уменьшить риск и серьезность инцидентов.

IV.A.3 Участие в деятельности механизмов по совместному использованию информации по наблюдению, предупреждению и реагированию на инциденты.

IV.A.4 Разработку, проверку и отработку планов, процедур и протоколов для чрезвычайных обстоятельств в целях создания условий доверия и эффективной координации деятельности правительственных и неправительственных органов в условиях кризиса.

IV.B Конкретные меры для достижения этих целей

Создание возможности национального управления инцидентами требует длительных усилий, которые начинаются с создания национальной группы реагирования на компьютерные инциденты (CIRT)[12, 13].

---

[12] См. Резолюцию 58 ВВУИО. В некоторых странах CIRT называется Национальной группой реагирования на инциденты, связанные с компьютерной безопасностью (NCSIRT) или Национальной группой реагирования на инциденты, связанные с безопасностью (N-SIRT).

IV.B.1 Определить или создать национальный потенциал CIRT.

1 Эффективное реагирование на существенные киберинциденты может ограничить ущерб, наносимый информационным системам, обеспечить действенные способы реагирования и сократить сроки восстановления и затраты на него. Совместно с государственным и частным секторами CIRT должна служить координационным пунктом в органах государственного управления, в особенности при инцидентах национального значения, для координации действий по защите от киберинцидентов и реагирования на них. В таких случаях CIRT должны сотрудничать с соответствующими органами, но не направлять и не координировать их деятельность.

2 Предполагается, что национальная CIRT будет предоставлять услуги и обеспечивать поддержку для предотвращения угроз в сфере кибербезопасности и реагирования на них, а также служить единым контактным центром для сообщения об инцидентах в сфере компьютерной безопасности, координации действий и связи. В задачи национальной CIRT должны входить анализ, предупреждение, совместное использование информации, снижение уязвимости, смягчение последствий и содействие принимаемым на национальном уровне мерам по восстановлению важнейшей информационной инфраструктуры. В частности, национальная CIRT должна выполнять на национальном уровне несколько функций, в том числе:

- выявление и идентификация аномальной деятельности;
- анализ угроз и аспектов уязвимости в сфере кибербезопасности, а также распространение предупреждений об угрозах в этой сфере;
- анализ и систематизирование информации об инцидентах и уязвимости, распространяемой другими лицами, в том числе поставщиками и экспертами по технологиям, для предоставления заинтересованным сторонам результатов оценки;
- создание надежных механизмов связи и содействие связи между заинтересованными сторонами для совместного использования информации и решения проблем кибербезопасности;
- обеспечение информации для раннего предупреждения, в том числе информации по уменьшению уязвимости и потенциальным проблемам;
- разработка стратегий смягчения последствий и реагирования и обеспечение скоординированного реагирования на инцидент;
- совместное использование данных и информации об инциденте и соответствующее реагирование;
- отслеживание и контролирование информации для определения тенденций и долгосрочных стратегий реагирования; и
- пропаганда передового опыта в сфере кибербезопасности в целом и обеспечение указаний в отношении реагирования на инциденты и их предотвращения.

IV.B.2 Создать в рамках органов государственного управления механизм(ы) координации деятельности гражданских учреждений, правоохранительных органов, структур обороны и разведки.

1 Одной из основных функций созданной на национальном уровне CIRT является распространение информации, в том числе информации о существующих аспектах уязвимости и угрозах, среди заинтересованных сторон. К числу заинтересованных сторон, которые должны участвовать в деятельности по реагированию, относятся соответствующие правительственные учреждения.

---

[13] Результаты работы, которые будут выполнены согласно Резолюции 58 МСЭ-Т могут затронуть Часть IV этих лучших принципов.

2 Эффективная координация с этими структурами может осуществляться в различных формах, включая поддержание веб-сайта для обмена информацией; предоставление информации через списки почтовой рассылки, в том числе информационные бюллетени, отчеты по тенденциям и результатам анализа; разработку публикаций, в том числе предупреждений, уведомлений и информации по различным аспектам кибербезопасности, включая новые технологии, аспекты уязвимости, угрозы и их последствия.

IV.B.3 Создать отношения сотрудничества с частным сектором для обеспечения готовности к киберинцидентам национального масштаба, их обнаружения, реагирования на них и восстановления после таких инцидентов.

1 Органы государственного управления и CIRT должны сотрудничать с частным сектором. Поскольку частный сектор во многих странах принадлежит значительная часть активов, относящихся к важнейшей информационной инфраструктуре и информационным технологиям, органы государственного управления должны действовать совместно с [частным сектором] для решения основной задачи – эффективного устранения инцидентов.

2 Отношения сотрудничества с частным сектором, основанные на доверии, дают органам государственного управления возможность получить представление о большей части важнейшей инфраструктуры, которая принадлежит частному сектору и эксплуатируется им. Частно-государственное сотрудничество может помочь в управлении рисками, связанными с киберугрозами, аспектами уязвимости и их последствиями, и добиться понимания ситуации посредством обмена информацией, информационно-пропагандистской работы и взаимодействия.

3 Стимулировать развитие практики обмена информацией между частным сектором и правительственными органами, создающей возможности для обмена оперативной информацией в режиме реального времени.

4 В число способов поощрения такого сотрудничества могут входить определение выгод, как для органов государственного управления, так и для частного сектора, разработка и реализация программ, обеспечивающих защиту секретных данных, являющихся собственностью компаний, создание рабочих групп, куда входили бы представители государственного и частного секторов, для управления рисками в киберпространстве и устранения инцидентов, обмен передовым опытом реагирования на инциденты/устранение инцидентов и учебными материалами, а также совместное определение функций и ответственности органов государственного управления и частного сектора в отношении устранения инцидентов в целях разработки, со временем, согласованных, предсказуемых протоколов.

IV.B.4 Создать контактный(ые) центр(ы) в рамках государственных учреждений, частного сектора и международных партнеров для содействия проведению консультаций, сотрудничеству и обмену информацией с CIRT.

1 Определение соответствующих контактных центров и установление рабочих отношений сотрудничества для консультаций, совместной работы и обмена информацией является основополагающим аспектом скоординированного и эффективного национального и международного механизма реагирования на инциденты. Эти взаимоотношения могут способствовать раннему предупреждению о возможных киберинцидентах и обмену информацией о тенденциях, угрозах и реагированию на них между структурами, занимающимися реагированием на инциденты, и другими заинтересованными сторонами.

2 Поддержание контактных центров и каналов связи с заинтересованными сторонами в состоянии, соответствующем современным требованиям, может способствовать активному и своевременному обмену информацией о тенденциях и угрозах и ускорять реагирование на них. Важно по мере возможности устанавливать контакты на основании служебных функций, а не на личных связях, с тем чтобы обеспечить, что каналы связи останутся открытыми, даже если то или иное лицо покинет организацию. Взаимоотношения часто

вначале основываются на доверии к конкретному лицу, но затем они должны преобразовываться в более официальные, институциональные договоренности.

IV.B.5 Участвовать в деятельности по международному сотрудничеству и обмену информацией.

1 Правительствам следует стимулировать сотрудничество с организациями, поставщиками и другими соответствующими экспертами в данной области, для того чтобы 1) ускорить реагирование на инциденты по всему миру; 2) продвигать и поддерживать возможности групп CIRT по присоединению к существующим глобальным и региональным конференциям и форумам, с целью создания потенциала для улучшения уровня реагирования на инциденты на региональном уровне; и 3) взаимодействовать по проблемам разработки материалов для создания национальных групп CIRT и для эффективного обмена информацией с руководствами CIRT.

IV.B.6 Разработать инструменты и процедуры для защиты киберресурсов государственных структур.

1 Для эффективного устранения инцидентов также необходима разработка и реализация направлений политики, процедур, методик, средств контроля в сфере безопасности и инструментов для защиты государственных киберактивов, систем, сетей и функций. Для CIRT это могут быть постоянно действующие инструкции (SOP), руководящие принципы для внутренних и внешних операций, направления политики безопасности для координации с заинтересованными сторонами, развертывания защищенных информационных сетей для операций CIRT и безопасной связи. В качестве координатора реагирования на инциденты CIRT должны координировать свои действия и способствовать сотрудничеству с другими структурами, ответственными за реагирование на инциденты. Органы государственного управления должны также обеспечивать на постоянной основе профессиональную подготовку по вопросам реагирования на инциденты для уже работающих и новых сотрудников.

IV.B.7 Создать с помощью CIRT потенциал для координации операций правительственных органов в целях реагирования на крупномасштабные кибернетические атаки и восстановления после них.

1 Если тот или иной инцидент вырастет до национальных масштабов, то потребуется главный координатор для координации деятельности с другими правительственными учреждениями, равно как и с другими заинтересованными сторонами, такими как частный сектор. Важно разработать планы и процедуры, позволяющие обеспечить готовность CIRT к устранению инцидента.

IV.B.8 Способствовать развитию практики ответственного раскрытия информации об уязвимых местах, для того чтобы обеспечить нормальное функционирование кибернетической инфраструктуры и защитить ее целостность.

1 Иногда могут обнаруживаться уязвимые места в продуктах информационных технологий, например в аппаратном и программном обеспечении. Решения о публичном раскрытии информации принимаются по каждому конкретному случаю в отдельности, с тем чтобы уязвимая информация не была использована злоумышленниками. Поставщикам должно быть предоставлено достаточно времени, прежде чем такая уязвимая информация может быть раскрыта.

ЧАСТЬ V

Содействие развитию национальной культуры кибербезопасности

С учетом того что персональные компьютеры становятся все более мощными, что происходит конвергенция технологий, что все шире распространяется применение ИКТ и что растет число соединений через государственные границы, все, кто разрабатывает, владеет, управляет, обслуживает и использует информационные сети, должны осознавать проблемы кибербезопасности и принимать соответствующие их функциям меря для защиты сетей. Органы государственного управления должны играть ведущую роль в создании культуры кибербезопасности и в поддержке мер, принимаемых другими участниками.

V.A Обзор цели, относящейся к настоящей части

V.A.1 Содействовать развитию национальной культуры безопасности согласно резолюциям 57/239 "Создание глобальной культуры кибербезопасности"[14] и 58/199 "Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур"[15] Генеральной Ассамблеи Организации Объединенных Наций.

1 Содействие развитию национальной культуры безопасности касается не только роли органов государственного управления в обеспечении эксплуатации и использовании информационных инфраструктур, в том числе систем, эксплуатируемых органами государственного управления, но и ведения информационно-пропагандистской работы в частном секторе, гражданском обществе и среди частных лиц. Точно так же это охватывает подготовку пользователей государственных и частных систем, дальнейшее укрепление безопасности и другие важные вопросы, такие как неприкосновенность частной жизни, спам и вредоносные программные средства.

2 По мнению ОЭСР, ключевыми факторами культуры безопасности на национальном уровне являются приложения и услуги электронного правительства и защита важнейших национальных информационных инфраструктур. В результате этого национальные администрации должны внедрять приложения и услуги электронного правительства, как для совершенствования своих внутренних операций, так и для предоставления услуг более высокого качества частному сектору и гражданам. Безопасность информационных систем и сетей должна рассматриваться не только с точки зрения технологий, но и включать такие элементы, как предотвращение рисков, управление рисками и повышение осведомленности пользователей. ОЭСР пришла к выводу, что деятельность по линии электронного правительства благотворно сказывается не только на государственной администрации, но и на частном секторе и частных лицах. По-видимому, инициативы, касающиеся электронного правительства, служат мультипликатором, содействующим распространению культуры безопасности.

3 Страны посредством совместной деятельности, предпочтительно подписав соглашение некоторого типа, должны принять междисциплинарный и многосторонний подход к кибербезопасности с участием множества заинтересованных сторон, а некоторые из них уже создают структуру управления высокого уровня для реализации национальной политики. Крайне важными считаются инициативы по повышению осведомленности и просвещению наряду с обменом передовым опытом, сотрудничеством между участниками и использованием международных стандартов.

---

14 http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf.

15 http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

4 Чрезвычайно важное значение для развития культуры безопасности имеет международное сотрудничество, а также региональные организации для облегчения взаимодействия и обменов.

V.B Конкретные меры для достижения этой цели

V.B.1 Реализовать план обеспечения безопасности для эксплуатируемых государством систем.

1 На первоначальном этапе для обеспечения безопасности эксплуатируемых государством систем органам государственного управления следует разработать и реализовать план обеспечения национальной безопасности. При подготовке этого плана необходимо изучить вопросы управления рисками, а также проектирования защиты и ее реализации. Периодически следует проводить переоценку плана и хода его реализации, с тем чтобы определить достигнутый прогресс и выявить сферы, где план или ход его реализации нуждаются в совершенствовании. В плане следует также предусмотреть положения, касающиеся устранения инцидентов, включая реагирование, наблюдение, предупреждение и восстановление, а также каналы обмена информацией. В план по обеспечению безопасности следует также включить меры, предусмотренные в пункте V.B.2 для подготовки пользователей этих государственных систем и сотрудничества между органами государственного управления, частным сектором и частным сектором по вопросам профессиональной подготовки в сфере безопасности и инициатив. Обеспечение информированности и ответственности пользователей является основной целью профессиональной подготовки.

V.B.2 Реализовать программы и инициативы по обеспечению информированности в сфере безопасности, рассчитанные на пользователей систем и сетей.

1 Эффективная национальная программа по обеспечению информированности в сфере кибербезопасности должна способствовать повышению информированности в сфере кибербезопасности среди населения и его основных групп, обеспечивать поддержание взаимодействия со специалистами в области кибербезопасности из правительственных органов для осуществления обмена информацией об инициативах, касающихся кибербезопасности, и быть ориентированной на развитие сотрудничества по вопросам кибербезопасности. При разработке программы по повышению информированности следует учитывать три функциональных компонента: 1) проведение разъяснительной работы среди заинтересованных сторон и обеспечение взаимодействия с ними, позволяющие обеспечить установление и поддержание отношений доверия между представителями частного сектора, правительственных органов и научного сообщества, в целях повышения информированности в сфере кибербезопасности и эффективной защиты киберпространства; 2) обеспечение координации, имеющей целью обеспечение сотрудничества при проведении мероприятий и деятельности в рамках правительственных органов; и 3) обмен информацией и сообщениями, ориентированный на развитие внутренних (в рамках правительственного учреждения, ответственного за данную программу) и внешних связей (с другими правительственными учреждениями, отраслью, учебными заведениями, пользователями бытовых компьютеров и населением).

V.B.3 Содействовать формированию культуры безопасности на коммерческих предприятиях.

1 Формирование культуры безопасности на коммерческих предприятиях может быть обеспечено с использованием нескольких инновационных способов. Многие государственные инициативы имеют целью повышение информированности среди малых и средних предприятий. Диалог правительства с ассоциациями деловых кругов или сотрудничество общественных и частных организаций с гражданами могут помочь административным органам в разработке и реализации инициатив в сфере просвещения и профессиональной подготовки. К примерам таких инициатив можно отнести: предоставление информации (в автономном и онлайновом режимах) – брошюр, пособий, руководств, образцов направлений политики и концепций; создание веб-сайтов, рассчитанных конкретно на МСП и другие заинтересованные стороны; организация профессиональной подготовки (в онлайновом режиме); обеспечение онлайнового механизма

самооценки; и предоставление финансовой помощи и налоговой поддержки или других стимулов для развития производства защищенных систем или принятие опережающих мер по усилению кибербезопасности.

V.B.4 Оказывать поддержку проводимой гражданским обществом информационно-пропагандистской работе, уделяя особое внимание потребностям детей и молодежи, лиц с ограниченными возможностями и индивидуальных пользователей.

1 Некоторые органы государственного управления сотрудничают с коммерческим сектором для повышения информированности граждан о появляющихся угрозах и о мерах, которые следует принимать для борьбы с ними. В ряде стран проводятся специальные мероприятия, такие как день, неделя или месяц информационной безопасности, и планируются различные виды деятельности по усилению информационной безопасности для широкой аудитории, в том числе населения. Большинство инициатив направлено на просвещение детей и учащейся молодежи либо посредством школьных механизмов, включающих учителей, преподавателей и родителей, либо путем непосредственной раздачи инструктивных материалов. Используются такие вспомогательные материалы, как веб-сайты, игры, онлайновые инструменты, открытки, учебники, а после сдачи экзаменов выдаются дипломы. К примерам таких инициатив можно отнести проведение учебных курсов для родителей с целью информирования их о связанных с безопасностью рисках; обеспечение учителей вспомогательными материалами; снабжение детей инструментами для онлайновых игр, в ходе которых они приобретают сведения по информационной безопасности; разработку учебников и игр; проведение экзамена и выдачу диплома: и проведение викторины о том, как безопасно путешествовать в сети.

2 Органы государственного управления и частный сектор могут обмениваться опытом, накопленным при разработке планов в сфере безопасности и подготовке пользователей; сообщать друг другу о достигнутых успехах и вводимых инновациях; и принимать меры для повышения безопасности внутренних информационных инфраструктур.

V.B.5 Содействовать разработке комплексной национальной программы повышения информированности, с тем чтобы все участники – коммерческие предприятия, все работающие в целом и все население – обеспечивали безопасность своих частей киберпространства.

1 Многие информационные системы уязвимы, потому что пользователи, системные администраторы, разработчики технологии, специалисты по закупкам, ревизоры, руководители информационных служб и советы директоров корпораций в недостаточной мере осведомлены о проблемах кибербезопасности. Эти аспекты уязвимости могут представлять серьезный риск для инфраструктур, даже не являясь собственно их частями. Например, степень понимания проблем безопасности системными администраторами зачастую представляет собой слабое звено в плане предприятия в сфере безопасности. Уменьшению этих аспектов уязвимости может помочь содействие принимаемым частным сектором мерам по подготовке персонала и принятие повсеместно признаваемых сертификатов по вопросам безопасности для персонала. Осуществляемая органами государственного управления на национальном уровне координация информационно-пропагандистской работы и повышения информированности для создания культуры безопасности поможет также добиться доверия со стороны частного сектора. Кибербезопасность – это общая ответственность. Порталы и веб-сайты могли бы стать эффективным механизмом содействия реализации национальной программы повышения информированности, благодаря которой государственные учреждения, коммерческие предприятия и индивидуальные потребители могут получать соответствующую информацию и принимать меры для защиты своих участков киберпространства.

V.B.6 Активизировать деятельность в области науки и техники и научно-исследовательские и опытно-конструкторские разработки (НИОКР).

1 В том случае, если органы государственного управления оказывают поддержку деятельности в области науки и техники и научно-исследовательским и опытно-конструкторским разработкам, часть предпринимаемых ими усилий должна направляться и

на обеспечение безопасности информационных инфраструктур. Определяя приоритеты НИОКР в киберпространстве, страны могут способствовать тому, чтобы при разработке продуктов проблемы безопасности учитывались, а сложные технические вопросы своевременно решались. Если НИОКР проводятся в академическом учреждении, то могут появиться возможности привлечения студентов к разработке инициатив в сфере кибербезопасности.

V.B.7 Проанализировать действующий режим обеспечения неприкосновенности частной жизни и модернизировать его для соответствия онлайновой среде.

1 При этом анализе следует учитывать механизмы обеспечения неприкосновенности частной жизни, принятые различными странами и международными организациями, в том числе ОЭСР. Директивы ОЭСР по защите неприкосновенности частной жизни и трансграничных потоков личных данных, принятые 23 сентября 1980 года, по-прежнему отражают достигнутый на международном уровне консенсус по общим директивам относительно сбора личной информации и обращения с нею. Устанавливая основные принципы, директивы играют важную роль, содействуя представителям органов государственного управления, коммерческих предприятий и потребителей в их усилиях по защите неприкосновенности частной жизни и личных данных, и устраняя не являющиеся необходимыми ограничения трансграничных потоков данных в автономном и онлайновом режимах.

V.B.8 Повышать информированность относительно кибернетических рисков и имеющихся решений.

1 Для решения технических проблем необходимо, чтобы органы государственного управления, коммерческие предприятия, гражданское общество и индивидуальные пользователи совместно занимались разработкой и реализацией мер, сочетающих *технологические* (стандарты), *процедурные* (применяемые в добровольном порядке директивы или обязательные регламентарные нормы) и *относящиеся к людским ресурсам* (передовой опыт) компоненты.

2 Одним из примеров угроз является спам и связанные с ним угрозы, такие как вредоносное программное обеспечение. Ряд организаций, включая Вопрос 4 ИК17 МСЭ-Т, работают по вопросам, касающихся спама. В Приложении A приведен краткий обзор высокого уровня этой проблемы.

3 Управление идентичностью является примером технологического инструмента для удовлетворения различных потребностей в области кибербезопасности. Ряд организаций, включая Вопрос 10 ИК17 МСЭ-Т, работают по вопросу управления идентичностью. В Приложении B приведен краткий обзор высокого уровня этой проблемы.

Дополнение 1

Список сокращений

APECTEL	Рабочая группа по электросвязи и информации Азиатско-Тихоокеанского экономического сотрудничества (АТЭС)
CAN-SPAM	Закон о контроле над рассылкой незапрошенных сообщений порнографического и маркетингового содержания от 2003 года (США)
CCIPS	Секции компьютерной преступности и интеллектуальной собственности (Министерство юстиции США)
CERT	Группа реагирования на нарушения компьютерной защиты
CERT-CC	Координационный центр групп реагирования на компьютерные инциденты (Университет Карнеги-Меллона, США)
CII	Важнейшая информационная инфраструктура
CIIP	Защита важнейшей информационной инфраструктуры
CIRT	Группа реагированию на компьютерные инциденты
COE	Совет Европы
CPNI	Центр по защите национальной инфраструктуры (Соединенное Королевство)
CVE	Перечень аспектов уязвимости и незащищенности (США)
DHS	Министерство национальной безопасности (США)
DOJ	Министерство юстиции (США)
EU	Европейский союз
FAR	Положение о федеральных закупках (США)
ФКС	Федеральная комиссия по связи (США)
FIRST	Форум групп по реагированию на инциденты и обеспечению безопасности
G8	Группа восьми (Объединенные Нации)
ИКТ	Информационно-коммуникационные технологии
ИМПАКТ	Международное многостороннее партнерство против киберугроз
ISAC	Центры обмена информацией и анализа информации (различные, такие как IT-ISAC; США)
IT-ISAC	Центр обмена информацией и анализа информации в области информационных технологий
ITAA	Американская ассоциация информационных технологий
ЛПД	Лондонский план действий
MSCM	Коммерческое сообщение электронной почты в среде подвижной связи
NIAC	Национальный консультативный совет по инфраструктуре (ITAA)
NIATEC	Национальный центр профессиональной подготовки и образования по вопросам обеспечения доступности, целостности и безопасности информации (при Университете Айдахо, США)
NIST	Национальный институт стандартов и технологий (США)
NRIC	Совет по надежности и совместимости сетей (ФКС США)

NSTAC	Национальный консультативный комитет по безопасности и электросвязи (DHS США)
NVD	Национальная база данных по вопросам уязвимости (США)
ОЭСР	Организация экономического сотрудничества и развития
OVAL	Открытый язык описания уязвимостей (Международный стандарт для распространения открытого и доступного контента, стандартизации и передачи информации по всему спектру средств и сервисов безопасности)
КТСОП	Коммутируемая телефонная сеть общего пользования
НИОКР	Научно-исследовательские и опытно-конструкторские работы
S&T	Наука и техника
МСП	Малые и средние предприятия
SMS	Служба коротких сообщений
SOP	Постоянно действующие инструкции
TCPA	Закон о защите прав потребителей телефонных услуг (США)
ГА ООН	Генеральная Ассамблея Организации Объединенных Наций

Дополнение 2

Национальная стратегия реализации сотрудничества в целях обеспечения кибербезопасности и показатели эффективности

Описанный ниже подход предусматривает использование методики, разработанной для того, чтобы страны могли создавать надежные системы кибербезопасности, что считается национальным приоритетом. Эта методика предусматривает три отдельных этапа программы, выполняя которые, страны пройдут путь от начального определения возможностей до реализации программы и ее оценки. Данный поэтапный подход представлен ниже:

Программная методика для сотрудничества в области кибербезопасности и показатели эффективности

Этап 1 – Определение, оценка и рекомендация плана совместной программы обмена.

- **Определение**: Первым шагом для страны является определение текущего состояния программы обеспечения безопасности. Этот этап выполняется группой экспертов при использовании стандартизированного инструмента оценки.
- **Оценка**: Информация, собранная в процессе определения, позволяет понять сильные и слабые стороны действующей в стране программы обеспечения кибербезопасности и определить вектор приложения усилий.
- **Рекомендация**: Видение ситуации, сформировавшееся в ходе оценки, является основой плана, который должен отвечать требованиям данной страны.

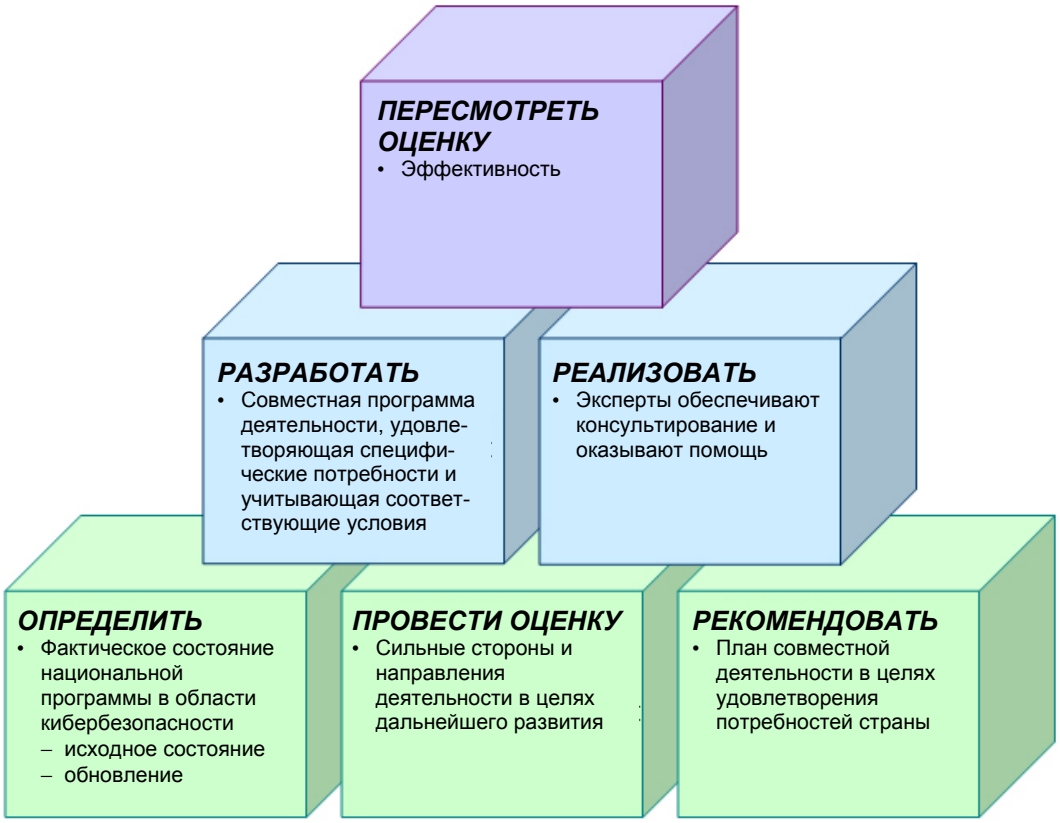
Этап 2 – Разработка и выполнение программы сотрудничества.

- **Разработка программы сотрудничества**: Проводится встреча экспертов страны на внутреннем уровне или с участием зарубежных партнеров, для того чтобы разработать план, наметить и скорректировать виды конкретной деятельности, необходимые для удовлетворения потребностей данной страны и учитывающие действующие в ней условия. Эти виды деятельности могут охватывать совместные мероприятия по обмену и определение долгосрочных потребностей в материалах.
- **Выполнение программы**: Эксперты на национальном уровне или, возможно, при участии зарубежных экспертов выполняют программу и вырабатывают конкретные рекомендации.

Этап 3 – Оценка программы сотрудничества для определения степени ее успешности и завершение выполнения программы.

- **Оценка программы сотрудничества**: Программа сотрудничества для обеспечения кибербезопасности регулярно подвергается переоценке на внутреннем уровне или при участии партнеров данной страны. Области, в которых выявлены недостатки, могут становиться объектом дальнейшего сотрудничества по обмену и выполнения вышеописанного процесса. Если страна сотрудничает с другими странами, такое сотрудничество можно будет завершить, если программа этой страны будет признана эффективной.

Рисунок 1: Программная методика для создания потенциала в области кибербезопасности



Показатели эффективности

Ниже представлен один из подходов к измерению результатов деятельности в этой области в динамике по времени и представлению достигнутых успехов руководству. Этот подход предусматривает построение логической цепочки, связывающей основные исходные данные (государственные или региональные программы, на выполнение которых расходуются время, денежные средства и кадровые ресурсы) с ожидаемым окончательным итогом (более высокий уровень кибербезопасности). Для иллюстрации этой цепочки используется следующая таблица:

Категория измерений:	**Компонент результата деятельности**:
Основные исходные данные:	**Программы стран**: • Время • Денежные средства • Кадровый состав
Основной рабочий процесс:	**Работа, включая возможное сотрудничество по обмену, в следующих областях**: • Разработка национальной стратегии • Разработка нормативно-правовой базы • Управление деятельностью при инцидентах • Сотрудничество общественных и частных организаций с гражданами • Культура кибербезопасности
Основные результаты деятельности:	**Количество**: • Совещаний или случаев обмена в рамках совместной деятельности

- Контактов с руководством политического и технического направлений

Промежуточные результаты:

Действия на уровне страны:

- Новые законы и нормативные акты в отношении киберпреступности
- Правоприменительные действия
- Создание CIRT
- Программы повышения осведомленности в рамках партнерств органов государственного управления и [частного сектора]
- Запросы относительно реагирования на инциденты
- Участие в проводимых международными организациями мероприятиях по кибербезопасности
- Выполнение международных конвенций и руководящих принципов

Конечный результат: Снижение уровня риска нарушения кибербезопасности, обусловленное национальной стратегией, законами в отношении киберпреступности, регламентарными нормами, рекомендуемыми руководящими принципами и более высоким уровнем самосознания потребителей.

Окончательный итог: Возросший уровень национальной кибербезопасности и глобальной безопасности.

Приложение A

Исследование: Спам

МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Серия X

Дополнение 6
(09/2009)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

Серия X.1240 МСЭ-Т – Дополнение по борьбе со спамом и связанными с ним угрозами

ПРЕДУПРЕЖДЕНИЕ!
НЕОПУБЛИКОВАННАЯ ВЕРСИЯ РЕКОМЕНДАЦИИ

Настоящая неопубликованная версия является неотредактированной версией недавно принятой Рекомендации. Она будет заменена опубликованной версией после редактирования. Поэтому между настоящей неопубликованной и опубликованной версией будут существовать различия.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ [не] получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

Дополнение 6 к Рекомендациям МСЭ-Т серии X

Серия X.1240 МСЭ-Т – Дополнение по борьбе со спамом и связанными с ним угрозами

Краткое содержание

В Дополнении 6 к Рекомендациям МСЭ-Т серии X утверждается, что для эффективной борьбы со спамом правительства должны использовать различные подходы, включая эффективные законы, технологические инструменты и обучать потребителей и организации. В настоящем дополнении описываются международные форумы, где обсуждается вопрос спама. В качестве учебного примера с целью иллюстрации в нем представлена определенная информация о способах, при помощи которых США и Япония подходят к проблеме спама.

Источник

Дополнение 6 к Рекомендациям МСЭ-Т серии X было согласовано 25 сентября 2009 года 17-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.)

СОДЕРЖАНИЕ

Дополнение 6 к Рекомендациям МСЭ-Т серии X

Серия X.1240 МСЭ-Т – Дополнение по борьбе со спамом и связанными с ним угрозами

1 Обзор

Темой настоящего дополнения является спам и связанные с ним угрозы. Настоящее дополнение предназначено для национальных администраций, которые не знакомы с понятием спама и хотели бы иметь основную информацию о нем.

В этом дополнении рассматриваются инструменты, которые следует применять для эффективной борьбы со спамом, и описывается работа, которую в этой области ведут некоторые международные форумы. В нем представлено в качестве учебного примера для иллюстрации описание того, что США и Япония предпринимают для борьбы со спамом.

2 Справочные документы

Нет.

3 Определения

В настоящем Дополнении используются следующие термины:

3.1 **фишинг**: Попытка обмануть человека, направляя его на неверный веб-сайт с целью хищения личной информации этого человека.

3.2 **спам**: Хотя не существует однозначно утвержденного определения спама, этот термин обычно применяется для описания нежелательных электронных массовых сообщений по электронной почте или отправкой мобильных сообщений (SMS, MMS).

4 Сокращения и акронимы

В настоящем дополнении используются следующие аббревиатуры:

ADSP	Author Domain Sending Practices		Технология подписи домена автора сообщения
APEC TEL	Asia-Pacific Economic Community – Telecommunication & Information Working Group		Рабочая группа по электросвязи и информации Азиатско-Тихоокеанского экономического сотрудничества (АТЭС)
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (U.S.)		Акт по управлению атаками нежелательной порнографии и маркетинга 2003 года (США)
CNSA	Contact Network of Spam Authorities (European Union)		Контактная сеть полномочных органов по спаму (Европейский союз)
DKIM	Domain Keys Identified Mail		Идентификация почты с использованием доменных ключей
FCC	Federal Communications Commission (U.S.)	ФКС	Федеральная комиссия по связи (США)
FTC	Federal Trade Commission (U.S.)		Федеральная торговая комиссия (США)
ISP	Internet Service Provider	ПУИ	Поставщик услуг интернета
JEAG	Japan Email Anti-abuse Group (Japan)		Японская группа по предотвращению злоупотреблений электронными сообщениями (Япония)
LAP	London Action Plan		Лондонский план действий

MAAWG	Messaging Anti-Abuse Working Group	Рабочая группа по предотвращению злоупотреблений сообщениями (Япония)
MMS	Multimedia Messaging Service	Служба мультимедийных сообщений
MSCM	Mobile Service Commercial Messages	Мобильные сервисные коммерческие сообщения
OECD	Organization for Economic Co-operation and Development	ОЭСР Организация экономического сотрудничества и развития.
OP25B	Outbound Port 25 Blocking	Блокировка выходного порта 25
SMS	Short Messaging Service	Служба коротких сообщений
SPF	Sender Policy Framework	Структура политики отправителей

5 Условные обозначения

Нет.

6 Основные положения

6.1 **Спам** из надоедливых сообщений, содержащих рекламные предложения, превратился в более серьезную проблему кибербезопасности. Например, спам может быть транспортом для мошенничества, распространения вредоносного программного обеспечения (ПО), например, вирусов и шпионских программ, и принуждения пользователей предоставлять частную информацию, которая затем может использоваться для совершения кражи идентичности (т. е. фишинга). Спамеры имеют преимущество в том, что они могут рассылать свои сообщения из любой точки мира любому человеку, расходуя на это очень небольшие средства. Это делает спам международной проблемой, которая должна решаться посредством международного сотрудничества.

6.2 **Фишинг** использует то преимущество, что благодаря основным свойствам системы электронной почты интернета[16], любой пользователь может отправить электронное письмо кому угодно, практически без какой-либо аутентификации. Фишинг является попыткой обмануть кого-нибудь, направив его на неверный веб-сайт с целью кражи личной информации этого человека. Фишинг существует, главным образом, потому что иногда люди ждут писем с популярных сайтов, и они просто не понимают, что это письмо пришло не с легального сайта. Так как в электронной почте существует мало возможностей для аутентификации, без внимательного изучения сообщения трудно определить является ли письмо настоящим. Такое внимательное изучение требует глубокого знания основных механизмов, используемых в сети.

Фишинг также существует потому, что большинству людей трудно проверить, являются ли веб-сайты, которые они посещают, законными. Иногда мы не внимательно смотрим на адрес URL веб-страницы, прежде чем ввести секретную информацию, а иногда мы даже не знаем, каким должен быть правильный URL-адрес.

Веб-серверы, применяемые для "фишинга" секретной информации, часто сами являются жертвами вредоносного ПО, что делает чрезвычайно сложным отслеживание фишеров.

6.3 **Вредоносное ПО**, или вредоносные программы, которые созданы для работы на устройстве без ведома или разрешения владельца, также представляет серьезную проблему.

7 Национальные подходы к эффективной борьбе со спамом и сопутствующими угрозами

7.1 **Национальная стратегия и спам**. В соответствии с национальной стратегией страны для эффективной борьбы со спамом должны создавать и поддерживать комбинацию эффективных

---

[16] Система электронной почты интернета была создана в 1970-е годы, когда доступ в интернет имело очень небольшое количество исследователей и членов правительства. Не было необходимости подтверждения идентичности человека, отправляющего электронное письмо, и потому не предпринимались попытки заставить систему это делать. Несмотря на то что система электронной почты с тех пор эволюционировала, это основное упущение остается до сих пор.

законов, органов и инструментов охраны правопорядка, технологических инструментов и лучших практик и обучение пользователей и бизнесменов.

7.2 Правовые и регуляторные принципы и спам. В соответствии с правовыми принципами и регуляторными основами органы управления, к чьей юрисдикции относится спам, должны иметь необходимые органы для расследования и принятия мер против нарушения законов, относящихся к спаму, которые совершаются в их стране или отражаются на ней. Органы власти, к чьей юрисдикции относится спам, также должны иметь механизмы для сотрудничества с иностранными органами власти. Обращения за помощью от иностранных органов управления должны рассматриваться в соответствии с областями общего интереса, и в тех случаях, когда наблюдается большой вред.

7.3 Совместная деятельность правительства и промышленности и повышение национальной осведомленности о спаме и сопутствующих угрозах. Все заинтересованные люди, включая органы охраны правопорядка, предприятия, промышленные группы и группы потребителей при преследовании нарушения законов, относящихся к спаму, должны действовать совместно. Правительственные органы охраны правопорядка должны сотрудничать с промышленными группами и группами потребителей с целью обучения пользователей и содействия в распространении информации. Правительственные органы охраны правопорядка должны сотрудничать с частным сектором с целью содействия в развитии технологических инструментов для борьбы со спамом, включая инструменты для облегчения обнаружения и идентификации спамеров.

Фишинг часто можно предотвратить. Правительства должны работать вместе с частным сектором для усовершенствования средств защиты граждан от фишинга и обучения потребителей и бизнесменов методам безопасной аутентификации.

Правительства также могут играть роль в обучении людей необходимости проверки вредоносного ПО, применяя такие инструменты как, например антивирусное ПО, и используя новейшие исправления для операционных систем и проверенные компьютерные технологии.

8 Международные (многосторонние) инициативы противодействия спаму

Несколько многосторонних форумов работают над инициативами борьбы со спамом. Они включают в себя:

8.1 Лондонский план действий

Федеральная торговая комиссия США (FTC) и Управление законной торговли Соединенного Королевства создали в Лондоне в 2004 году Международную конференцию соблюдения законов о спаме, что привело к созданию Лондонского плана действий по международному сотрудничеству по соблюдению законов о спаме (LAP). На июль 2008 год правительственные органы и представители частного сектора из более, чем 25 стран, одобрили этот план. LAP содействует заинтересованным сторонам, включая органы по борьбе со спамом и участников из частного сектора, в рассмотрении заявок на членство в организации.

Целью LAP является развитие международного сотрудничества в борьбе со спамом и работе с проблемами, сопутствующими спаму, например онлайновое мошенничество и обман, фишинг и распространение вирусов. LAP строит взаимоотношения между этими объектами на основе короткого документа, в котором излагается основной рабочий план усиления международной борьбы и сотрудничества в обучении против нелегального спама. Этот документ не является обязательным и просит участников только предпринять максимум возможного для продвижения рабочего плана. http://londonactionplan.org/.

С самого начала в рамках LAP проводятся ежегодные семинары, обычно вместе с Контактной сетью полномочных органов по спаму Европейского союза (CNSA). В октябре 2007 года LAP и CNSA провели свой ежегодный совместный семинар вместе с Конференцией Рабочей группы по предотвращению злоупотреблений сообщениями (MAAWG), проходящей в Арлингтоне, Вирджиния, что облегчило усиленное сотрудничество с частным сектором по правоприменению. В октябре 2008 года, LAP и CNSA провели своей ежегодный совместный семинар вместе с 6-м Совещанием по борьбе со спамом Eco в Германии в Висбадене, Германия.

8.2 Инструментарий ОЭСР по борьбе со спамом и Рекомендация Совета по сотрудничеству в борьбе со спамом

В апреле 2006 года Специальная комиссия по спаму ОЭСР выпустила "Инструментарий" по борьбе со спамом, который содержит рекомендации, помогающие создателям правил, органам управления и участникам промышленного сектора отлаживать свои правила борьбы со спамом и восстановить доверие к интернету и электронной почте. Инструментарий содержит восемь элементов, включая нормативные документы по борьбе со спамом, решения, созданные промышленностью, и антиспамовые технологии, обучение и информированность, и международное сотрудничество/программа помощи. Учитывая, что международное сотрудничество является основой для борьбы со спамом, правительства ОЭСР также утвердили "Рекомендацию по международному сотрудничеству в применении законов портив спама", которая побуждает страны давать гарантии того, что их законы позволяют органам охраны правопорядка делиться информацией с другими странами и делать это более эффективно и быстро. http://www.OECD-antispam.org/sommaire.php3

8.3 Симпозиум APEC TEL по спаму

В апреле 2006 года, APEC TEL провела симпозиум по "Спаму и сопутствующим угрозам", в котором участвовало тридцать докладчиков и участников дискуссии, для обсуждения развития проблемы спама и создания общего плана действий для TEL. Основные обсуждавшиеся темы включали:

1) создание и применение национальных регламентарных систем борьбы со спамом, включая соблюдение законов и процессуальных кодексов;

2) роль промышленности в борьбе со спамом, включая сотрудничество между правительством и промышленностью;

3) технические методы реагирования на спам;

4) международное сотрудничество и соблюдение законов, включая Конвенцию о киберпреступности Европейского союза и Рекомендацию совета ОЭСР по сотрудничеству в соблюдении законов, как основных инструментов для усиления сотрудничества; и

5) необходимость направленного обучения пользователей и увеличения осведомленности.

Конкретные шаги TEL направленные на развитие, включают:

1) поддержку совместного использования информации по нормам и правилам, полученным из таких источников, как Инструментарий ОЭСР по борьбе со спамом;

2) создание список рассылки для органов борьбы со спамом АТЭС для добавления схожих источников, созданных ОЭСР и МСЭ;

3) поддержку экономики для применения в форумах добровольного сотрудничества в рамках членства, например Лондонский план действий или Соглашение Сеул-Мельбурн;

4) сотрудничество с ОЭСР по совместному использованию информации и инициативам, связанным с руководством; и

5) поддержку создания объема для развивающихся экономик для лучшей борьбы со спамом.

9 Исследование конкретных случаев деятельности по борьбе со спамом

В данном пункте рассматривается деятельность по борьбе со спамом в некоторых странах.

9.1 Соединенные Штаты Америки

9.1.1 Законодательные требования для лиц, рассылающих коммерческие электронные письма (Акт CAN-SPAM)

В 2003 году Соединенные Штаты утвердили "Акт CAN-SPAM", в котором установлены требования для лиц, рассылающих рекламные электронные письма, разъясняет наказания для спаммеров и компаний, чья продукция рекламируется в спаме, если они нарушают закон, и дает пользователям право попросить отправителей электронных писем прекратить отправку им спама.

Основные положения Акта CAN-SPAM включают:

- **Запрещение ложной или вводящей в заблуждение информации в заголовке**: "От", "Кому" и маршрутной информации вашей электронной почты – включая имя домена происхождения и адрес электронной почты – должны быть верными и определять лицо, отправившее электронное письмо.
- **Запрет ложных строк "тема"**: Строка "тема" не может вводить получателя в заблуждение касательно информационного содержимого или темы сообщения.
- **Требуется, чтобы ваше электронное письмо давало адресату способ отказа**: Вы должны предоставить обратный электронный адрес или любой механизм ответа на основе интернета, который позволяет отправителю попросить вас в будущем не отправлять электронные письма на этот электронный адрес, а вы должны удовлетворить запрос. Вы можете создать "меню" выбора, чтобы позволить адресату отказаться от определенного типа сообщений, но вы должны включить возможность прекратить любые коммерческие сообщения от отправителя. Любой механизм отказа, который вы предлагаете, должен быть способен обрабатывать запросы отказа в течение минимум 30 дней после отправки вами коммерческого электронного сообщения. Когда вы получаете запрос отказа, закон дает вам 10 рабочих дней для прекращения отправки электронных писем на адрес электронной почты запросившего адресата. Вы не можете помогать третьей стороне отправлять электронные письма на тот адрес, или просить третью сторону отправлять электронные письма на этот адрес от вашего лица. Наконец, вы не имеете законного права продавать или передавать адреса электронной почты людей, которые предпочли не получать ваши электронные письма, даже в виде списка рассылки, если вы передаете адреса так, что другое лицо может действовать в соответствии с законом.
- **Требуется, чтобы рекламные электронные письма определялись как реклама и содержали действующий физический почтовый адрес отправителя**: Ваше сообщение должно содержать четкое и заметное указание на то, что это сообщение является рекламой или навязыванием услуг, чтобы получатель мог отказаться дальше получать от вас коммерческие электронные письма. Также оно должно содержать ваш действующий физический почтовый адрес.

Федеральная торговая комиссия США (FTC) имеет право использовать свои гражданские органы правопорядка для обеспечения соблюдения правил Акта CAN-SPAM и для получения гражданских штрафов в размере до 11 000 долл. США за преступление. С 1997 года, когда FTC предприняло первое действие по соблюдению закона в отношении нежелательного коммерческого сообщения, или "спама," FTC активно преследовало ложные и нечестные действия спама в 94 процессах по соблюдению закона, 31 из которых были направлены против нарушителей Акта CAN-SPAM.

CAN-SPAM также дает Министерству юстиции США право усиливать его уголовные санкции. Акт CAN-SPAM предусматривает серьезное уголовное наказание, включая тюремное заключение для спаммеров. Другие федеральные органы и органы штатов могут также требовать соблюдения законов от организаций, находящихся в их юрисдикции, и компаний, которые предоставляют доступ в интернет преступникам.

9.1.2 Правила, запрещающие отправку коммерческих электронных писем на беспроводные устройства

В Соединенных Штатах также приняты правила, защищающие абонентов от получения нежелательных рекламных сообщений (спама) на свои беспроводные устройства. С некоторыми исключениями эти правила запрещают отправку рекламных электронных почтовых сообщений, включая электронные письма и определенные текстовые сообщения, на беспроводные устройства, например, сотовые телефоны. Эти правила применимы только к сообщениям, соответствующим определению "рекламное", используемому в Акте CAN-SPAM, – и к тем сообщениям, когда главной задачей сообщения является рекламное объявление или предложение коммерческого продукта или услуги. Некоммерческие сообщения, например, сообщения о кандидатах на публичную должность, или сообщения, извещающие существующего абонента об изменениях на его или ее счете, правилами не рассматриваются.

Мобильные сервисные рекламные сообщения (MSCM) включают в себя любые рекламные сообщения, отправленные на адрес электронной почты абонента, и происходящие от поставщика услуг мобильного беспроводного устройства. MSCM запрещены, если только отдельные адреса предоставлены отправителю до авторизации (известно, как требование "рассылки по запросу"). Это

правило запрещает отправку любого рекламного сообщения на адреса, содержащие доменные имена, указанные в списке ФКС минимум за 30 дней или в любое время, превышающее срок 30 дней, если отправитель знает, что сообщение адресовано на беспроводное устройство. Для того чтобы помочь отправителям рекламных сообщений определить, какие адреса принадлежат беспроводным абонентам, правила требуют, чтобы поставщики беспроводных услуг предоставляли Федеральной комиссии по связи (ФКС) названия соответствующих доменных почтовых имен. Сообщения службы коротких сообщений (SMS), передаваемые только на телефонные номера, не имеют этой защиты. Вызовы с автонабором уже защищаются другими законами.

В рамках правил ФКС, ФКС может налагать на спаммеров денежные штрафы от 11 000 долл. США за нарушение, связанное с отсутствием лицензии, до 130 000 долл. США за нарушение, связанное с лицензированием линии связи. Кроме денежных штрафов ФКС может издать постановление о приостановке или прекращении работы спамера, который нарушил любое положение Закона о связи или любое правило ФКС, утвержденное Актом. Дополнительно в рамках Закона о связи любой нарушающий положение Закона, является объектом уголовного преследования Министерством юстиции (дополнительно к денежному штрафу) и может быть заключен под стражу на срок до 1 года (или двух при повторении преступления). На этот момент ФКС не инициировало ни одного судебного процесса по таким коммерческим сообщениям.

9.1.3 Подходы к ограничению фишинга

Как обсуждалось ранее основное предположение относительно того, на что рассчитывают спамеры и фишеры – это недостаток знаний того, кем является отправитель. Целевая группа по инженерным проблемам интернета (IETF) выпустила два стандарта, Идентификация почты с использованием доменных ключей (DKIM) [b-IETF RFC 4871] и Технология подписи домена автора сообщения (ADSP) [b-IETF RFC 5617], которые улучшают возможности адресата идентифицировать отправителей. Поставщики начали делать внедрения, доступные пользователям. Кроме того, существует, как минимум, одна доступная и свободная[17] реализация стандарта. Источником содействия является Рабочая группа по предотвращению фишинга (APWG), промышленная ассоциация, ориентированная на прекращение кражи идентичности и обмана, которые происходят из-за растущих проблем с фишингом и спуфингом электронной почты. Эта организация создала форум для обсуждения вопросов фишинга, задач и оценки возможных технологических решений, и доступа к централизованному хранилищу сведений о случаях фишинга (http://www.antiphishing.org).

Этот стандарт позволяет "утверждение белого списка", или способности подтвердить, что, например, это действительно ваш банк, или ваши друзья, или партнеры пытаются связаться с вами. Этот стандарт, по сути, и сам по себе ограничит некоторые виды фишинга, но не все.

9.2 Япония

9.2.1 Правоприменение

В Японии существуют два закона, ограничивающих отправку электронных сообщений в целях устранения спама, рассылаемого с использованием электронных сообщений. Ниже приводятся основные элементы данных законов.

- К отправке рекламных сообщений по электронной почте применяются следующие правила. (Согласие)
  - Отправка рекламных сообщений по электронной почте без согласия адресата на их получение запрещена.
  - Организационная структура отправителя должна хранить доказательства согласия получателей при отправке им рекламных сообщений.
  - В рекламных сообщениях должна содержаться информация о процедуре прекращения отправки рекламных сообщений, имя отправителя и т. д.

---

[17] "Свободная" здесь относится к способности ввести это свойство беспошлинно в условиях, определенных владельцем патента.

  - Если получатель правильно выполнит процедуру уведомления соответствующей организации о своем нежелании получать рекламные сообщения, то эта организация больше не может направлять рекламные сообщения данному получателю.

– Отправка электронных сообщений, содержащих фальшивую информацию об их отправителе, например фальшивые адреса электронной почты, IP-адреса и наименования доменов, запрещена.

– Отправка электронных сообщений по вымышленным адресам получателей, автоматически создаваемым компьютерной программой, запрещена.

9.2.2 Совет по содействию мерам по борьбе со спамом

Самые различные заинтересованные стороны, а именно: ПУИ, рекламодатели, поставщики службы приложений для доставки рекламных сообщений, поставщики защитных средств, организации потребителей, органы управления и т. д., создали в 2008 году Совет по содействию мерам по борьбе со спамом. В ноябре 2008 года Совет принял "Декларацию о мерах по искоренению спама".

9.2.3 Центр киберконтроля (CCC)

В результате тесного сотрудничества между японским правительством, организациями, связанными с ПУИ, и основными ПУИ, был создан центр киберконтроля (CCC), занимающийся выявлением ПК, зараженных ботами. Центр работает следующим образом.

– CCC управляет большой системой "honey pot", которая получает информацию от ПК, заражениях вирусом (обычно ботом). Система "honey pot" собирает IP-адреса заражающих ПК и коды вредоносных программ (ботов).

– Перечни IP-адресов, а также дат/времени их обнаружения направляются каждому ПУИ. Каждый ПУИ выявляет своих абонентов, имеющих эти IP-адреса, и информирует их о том, что их ПК могут быть заражены вредоносным программным обеспечением. Кроме того, каждый ПУИ направляет им информацию о CCC (ссылка на соответствующую веб-страницу) и программное обеспечение для удаления вирусов.

– CCC анализирует полученные коды программ. Если соответствующий код программы ранее не идентифицировался, то создается и выпускается новое программное обеспечение для удаления вирусов, которое может обеззаразить код этой новой вредоносной программы.

Эта работа способствует пресечению деятельности, связанной с заражением ботами в Японии. Ввиду того, что большинство электронных сообщений, содержащих спам, рассылаются с ПК, зараженных ботами, то это также приводит к уменьшению отправок из Японии электронных сообщений, содержащих спам.

9.2.4 Блокировка выходного порта 25 (OP25B)

Когда абоненты ПУИ отправляют или получают электронные сообщения, они пользуются услугой электронной почты, которая обычно предоставляется ПУИ. Поэтому абоненты отправляют свои электронные сообщения на почтовые серверы своего ПУИ, которые передают эти сообщения на серверы электронной почты адресата. Абоненты ПУИ обычно не отправляют свои электронные сообщения напрямую на серверы электронной почты адресата. А поскольку зараженные ботом или вирусом ПК отправляют сообщения, содержащие спам, напрямую по адресу серверов электронной почты адресата, то такие электронные сообщения не проходят через почтовые серверы соответствующего ПУИ. Если удастся остановить сообщения, поступающие с ПК абонентов в обход сети ПУИ, использующей SMTP (протокол управления передачей (TCP) с номером порта 25 пункта назначения), то можно заблокировать многие сообщения, содержащие спам. Поэтому японское правительство, ПУИ и связанные с ними организации внимательно изучили следующие вопросы в тесном сотрудничестве друг с другом.

– Какое влияние на абонентов оказывает введение блокировки выходного порта 25 TCP (OP25B) [b-MAAWG MP25].

– Ограничения в отношении блокировки специальных сообщений согласно действующему японскому законодательству.

После проведения этих исследований многие ПУИ применяют OP25B при осуществлении своей деятельности. JEAG (Японская группа по предотвращению злоупотреблений электронными сообщениями) играет важную роль в этом процессе, публикуя рекомендации для ПУИ с настоятельным призывом внедрения OP25B.

– Хотя внедрение OP25B не является обязательным для японских ПУИ, 52 ПУИ, в том числе почти все основные ПУИ, к июлю 2009 года внедрили OP25B.

– Многие ПУИ, внедряющие OP25B, обеспечивают порт 587 TCP SMTP AUTH, в качестве альтернативного способа связи, без ухудшения качества обслуживания. Пользователи могут отправлять электронные сообщения от другого ПУИ, адаптируя OP25B к почтовому серверу этого ПУИ.

9.2.5 Технологии аутентификации отправителя

Технологии аутентификации отправителя – это методы обнаружения подмены адреса источника электронного сообщения. JEAG опубликовала рекомендацию для внедрения этого метода, а министерство внутренних дел и связи опубликовало документ “Важные правовые вопросы, касающиеся внедрения аутентификации отправителя на принимающей стороне ПУИ”. В настоящее время практически все крупные операторы подвижной связи и некоторые ПУИ внедрили структуру политики отправителей (SPF) [b-IETF RFC 4408], одну из технологий аутентификации отправителя, и теперь их абоненты могут использовать результаты аутентификации для фильтрации. Доля опубликованных записей SPF для доменов "jp" составляла в августе 2009 года 35,99%. Кроме того, несколько ПУИ начали внедрять DKIM [b-IETF RFC 4871], в качестве дополнительного способа аутентификации отправителя.

9.2.6 Обмен информацией об отправителях электронных сообщений, содержащих спам, между операторами подвижной связи

Почти все сотовые телефоны в Японии имеют возможность обработки обычных электронных сообщений. Поскольку большинство электронных сообщений, содержащих спам, отправляются в Японии с мобильных сотовых телефонов, то все операторы подвижной связи обмениваются информацией об отправителях сообщений, содержащих спам, следующим образом.

– Согласно "Закону о предотвращении ненадлежащего использования мобильного телефона", идентичность любого лица, желающего заключить контракт на пользование мобильными телефонами, проверяется.

– Если оператор подвижной связи выявляет пользователя сотового телефона, который отправляет электронные сообщения, содержащие спам, в нарушение "Закона о регулировании передачи указанных электронных сообщений", то информация о таком пользователей сообщается всем остальным операторам подвижной связи.

Поэтому, если тот или иной пользователь отправляет электронные сообщения, содержащие спам, с сотового телефона, то ему будет трудно получить контракт на использование мобильного телефона в Японии.

Одна соответствующая некоммерческая организация устанавливает сенсорные устройства, собирает сообщения, содержащие спам, и анализирует их. Она предоставляет информацию об отправителях электронных сообщений, содержащих спам, соответствующим ПУИ в Японии и обменивается этой информацией с некоторыми агентствами в зарубежных странах.

Библиография

[b-IETF RFC 4871] IETF RFC 4871 (2007), *Подписи для идентификации почты с использованием доменных ключей (DKIM)*. http://www.ietf.org/rfc/rfc4871.txt

[b-IETF RFC 5617] IETF RFC 5617 (2009), *Технология подписи домена автора сообщения (ADSP) для идентификации почты с использованием доменных ключей (DKIM)*. http://www.ietf.org/rfc/rfc5617.txt

[b-MAAWG MP25] Рекомендация MAAWG (2005 г.), *Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction*. http://www.maawg.org/port25

[b-IETF RFC 4408] IETF RFC 4408 (2007), *Структура политики отправителей (SPF) для санкционирования использования доменов в электронной почте, версия 1*. http://www.ietf.org/rfc/rfc4408.txt

[b-contr-spam] "Закон о контроле за агрессивными массовыми рассылками порнографического и коммерческого характера 2003 года" (свод законов США). Этот закон документально подтвержден в следующих законах: 15 U.S.C. §§ 7701-7713; 18 U.S.C. § 1037; 28 U.S.C. § 994; 47 U.S.C. § 227. http://www.gpsaccess.gov/uscode/index.html

[b-ITU-T cyb] Отчеты о конференциях рабочей группы по противодействию злонамеренному использованию услуг передачи сообщений: http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html.

Приложение B

Управление индентичностью

МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Серия X

Дополнение 7
(02/2009)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Серия X.1250 МСЭ-Т – Дополнение к обзору управления идентичностью в контексте кибербезопасности

ПРЕДУПРЕЖДЕНИЕ!
НЕОПУБЛИКОВАННАЯ ВЕРСИЯ РЕКОМЕНДАЦИИ

Настоящая неопубликованная версия является неотредактированной версией недавно принятой Рекомендации. Она будет заменена опубликованной версией после редактирования. Поэтому между настоящей неопубликованной и опубликованной версией будут существовать различия.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ [не] получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

Дополнение 7 к Рекомендациям МСЭ-Т серии X

Серия X.1250 МСЭ-Т –Дополнение к обзору управления идентичностью в контексте кибербезопасности

Краткое содержание

Безопасность традиционной коммутируемой телефонной сети общего пользования (КТСОП) исследуется в течение многих десятилетий работы. Однако то же самое нельзя сказать о распространенных сетях передачи данных общего пользования с коммутацией пакетов с поставщиками множества услуг, например, интернет и сетей последующего поколения (СПП). Такие сети используют одну общую транспортную платформу для управления трафиком и для трафика пользователя, которая, помимо возможной анонимности такого трафика и возможности создания однонаправленного трафика, делает такие сети уязвимыми для злоупотребления. Все электронные услуги (е-услуги, например, электронный бизнес, электронная торговля, электронное здравоохранение, электронное правительство) открыты для атак. Эта проблема может быть, как минимум, частично решена путем улучшения секретности в идентичности пользователя, сетевых устройств и поставщиков услуг, так что они могут быть подтверждены, проверены и смогут получить соответствующий доступ. Так как управление идентичностью дает больше уверенности и доверия к идентичности пользователя, поставщика услуг и сетевых устройств, оно усиливает безопасность, уменьшая незащищенность от рисков безопасности. Этот аспект кибербезопасности является тем, что поставщики услуг должны учитывать на деловом и техническом уровне, и что правительства должны учитывать на национальном уровне, как часть плана национальной кибербезопасности.

Введение

Управление идентичностью (IdM) является способом управления и контроля информации, которая используется в процессе общения для представления объектов (например, поставщиков услуг, организаций конечного пользователя, сетевых устройств, программных приложений и услуг). Один объект может иметь множество цифровых идентичностей, чтобы иметь доступ к разным услугам с отличающимися требованиями, и они могут существовать во многих местах.

IdM является ключевым компонентом кибербезопасности, так как оно обеспечивает возможность создания и поддержки надежных линий связи между объектами. IdM поддерживает аутентификацию объекта. Оно также позволяет авторизацию ряда прав (вместо прав все-или-ничего) и делает проще изменение прав, если роль объекта изменяется. IdM также увеличивает способность организации применять ее правила безопасности, позволяя наблюдать и контролировать деятельность объекта в сети. IdM может обеспечить доступ к объектам как внутри, так и вне организации. Одним словом, хорошее решение IdM дает возможность поддержки аутентификации, обеспечения и управления идентичностями и проверки деятельности объекта.

IdM является важным компонентом в управлении безопасностью и обеспечении кочующего доступа по запросу к сетям и электронным услугам. Вместе с защитными механизмами, например, брандмауэрами, системами определения вторжения, защитой от вирусов, IdM играет важную роль в защите информации, линий связи и услуг от киберпреступлений, например мошенничество и кража идентичности. Одним из следствий из этого является то, что будет расти уверенность пользователей в том, что электронные транзакции будут безопасны и надежны. В свою очередь это увеличит желание пользователей использовать IP-сети для электронных услуг.

При создании системы IdM, нужно иметь в виду основные проблемы безопасности. Это означает необходимость разработки методов, которые гарантировали бы точность информации об идентичности, необходимость предотвращения возможности применения информации об идентичности в целях, выходящих за рамки того, для чего она была собрана.

1 Обзор

Управление идентичностью стало важным компонентом, который повысит безопасность, за счет обеспечения более точных гарантий, подтвердив достоверность информации об идентичности. В настоящем Дополнении представлен общий обзор этой новой услуги.

Использование термина "идентичность" в настоящем дополнении по отношению к IdM не отражает его полного значения. В частности, оно не составляет любого положительного подтверждения.

2 Справочные материалы

Нет.

3 Определения

Определения содержатся в других Рекомендациях серии X.1250.

4 Сокращения и аббревиатуры

IdM	Identity Management		Управление идентичностью
IP	Internet Protocol		Интернет протокол
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования

5 Условные обозначения

Нет.

6 Важность IdM для защиты инфраструктуры глобальной сети и многонациональной координации безопасности

Надлежащая реализация и использование возможностей и правил IdM в различных национальных, региональных и международных сетях повысит безопасность инфраструктуры глобальной сети. Лучшие реализации и действия IdM важны и необходимы для обеспечения гарантий информации об идентичности, а также целостности и доступности инфраструктуры глобальной сети.

Возможности IdM могут использоваться для поддержки национальных и международных услуг электросвязи в экстренных ситуациях за счет идентификации пользователей, имеющих доступ к определенным услугам.

Кроме того, возможности IdM могут применяться для предотвращения, обнаружения и поддержки координации действий по реагированию на национальные и международные инциденты в области кибербезопасности. В отдельных случаях IdM может помочь органам власти и организациям в деле координации их попыток по отслеживанию и обнаружению источника таких инцидентов.

7 Управление идентичностью, как средство для создания надежной связи между двумя объектами

Одной из важных функций IdM является аутентификация пользователей, сетей или услуг. В процессе аутентификации, включающем два объекта, один объект заявляет другому о своей идентичности. В зависимости от требований безопасности второго объекта, может потребоваться подтвердить это заявление прежде, чем второй объект будет доверять первому настолько, чтобы предоставить ему права. Выполнение этих процедур может потребоваться в обоих направлениях.

Существуют разные уровни доверия аутентификации, "немного-или-ничего", слабое (например, имя пользователя и пароль) и заканчивая сильным (например, инфраструктура с открытым ключом (МСЭ-Т X.509)). Оценка рисков может определить соответствующий уровень аутентификации. Для одного объекта может потребоваться более высокий уровень аутентификации, чем для другого, например, из-за того, что один объект управляет важными источниками.

8 Защита, поддержка, отмена и управление данными об идентичности

Другими важными функциями IdM являются защита, поддержка и управление надежными данными об идентичности, включая способность устанавливать текущий статус идентичности.

Законы или правила могут потребовать, чтобы информация, подлежащая личной идентификации, была защищена, и чтобы не допускалось использование информация об идентичности для целей, выходящих за рамки того, для чего она была собрана. Гарантии того, что данные об идентичности все еще действительны, являются еще одним важным вопросом. Для услуг, применение которых жизнеспособно, данные об идентичности должны соответствующим образом поддерживаться так, чтобы они были точны, своевременны и совместимы.

Там, где это важно, управление атрибутами данных об идентичности должно предусматривать возможность проверки, не отменены ли данные об идентичности.

Во многих случаях объектам потребуется возможность управления использованием своих собственных данных и личной информации.

9 "Обнаружение" надежных источников данных об идентичности

IdM также включает в себя понятие "обнаружения" надежных данных об идентичности. В среде с множеством чрезвычайно широко рассредоточенных поставщиков услуг (например, интернет и сети последующих поколений), данные об идентичности, требуемые для того, чтобы обеспечить доверие к идентичности и связанным с ней утверждениям объекта, могут находиться в разных местах в сети. Объекты могут иметь множество цифровых идентичностей с разными источниками информации об идентичности в разных местах. Когда один из двух объектов в процессе аутентификации перемещается, другому объекту потребуется обнаружить и установить надежную связь с

соответствующим источником информации об идентичности, чтобы завершить процесс аутентификации кочующего объекта. Концепция обнаружения источников надежной информации сходно с тем, что сегодня происходит при использовании мобильного сотового телефона.

10 Службы электронное правительство (службы e-government)

Преимущества для объекта от реализации IdM включают в себя снижение рисков, увеличение надежности, улучшенную функциональность и возможность снижения затрат. Эти причины для реализации IdM равно правомочны, когда объектом является правительство. В службах e-government главными задачами тоже являются снижение стоимости и предоставление более результативных и эффективных услуг гражданам и деловым партнерам правительства.

Как и другие объекты, правительства сталкиваются с вопросом как результативно и эффективно использовать идентичность в объединенном сетями мире. Для того чтобы реализовать службы e-government, правительство должно провести анализ рисков в электронных услугах, которые оно собирается предложить, и внедрить подходящие меры защиты. Важность многих служб e-government (например, e-health) может потребовать, чтобы правительство требовало сильной системы аутентификации.

11 Соображения по поводу законодательства в отношении IdM

Национальные администрации и региональные группы должны рассмотреть ряд возможных вопросов по законодательству в отношении реализации IdM, например, защита секретности и данных, национальная безопасность и готовность к чрезвычайным ситуациям, а также обязательные соглашения между операторами. Правительства не просто применяют методы управления идентичностью, но также могут применять их по отношению к другим объектам, с тем чтобы выполнить широкий спектр национальных правил и задач безопасности.

Библиография

По вопросам IdM работает множество форумов. Они включают в себя:

ARK (Ключ архивных ресурсов цифровой библиотеки Калифорнии): http://www.cdlib.org/inside/diglib/ark/

3GPP SA3: http://www.3gpp.org/SA3-Security?page=type_urls

ETSI TISPAN WG7: http://www.etsi.org/tispan/

EU eID Roadmap: http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

Европейская Карта Гражданина: http://europa.eu.int/idabc/servlets/Doc?id=19132

FIDIS (Будущее идентичности в информационном обществе ЕС): http://www.fidis.net/

FIRST (Форум команд реагирования на инциденты и безопасности): http://www.first.org/

Проектное руководство (Идентификация пользователя правительства ЕС для Европы): http://www.ist-world.org/ProjectDetails.aspx?ProjectId=4ddb2e61c84343f0acd370607e5a8499&SourceDatabaseId=7cff9226e582440894200b751bab883f

Handle: http://www.handle.net/

Higgins: http://www.eclipse.org/higgins/index.php

IDSP (Комитет Американского национального института стандартизации по предотвращению кражи идентичности и стандартам управления идентичностью (IDSP)): http://www.ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3

IGF (Основы управления идентичностью ORACLE): http://www.oracle.com/technology/tech/standards/idm/igf/index.html

ITRC (Центр ресурсов по краже идентичности): http://www.idtheftcenter.org/

Рабочая группа по инженерным вопросам интернета: http://sec.ietf.org/

17-я Исследовательская комиссия МСЭ-Т (Безопасность) Целевая группа по IdM: www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

17-я Исследовательская комиссия МСЭ-Т (Безопасность) Вопрос 10: http://www.itu.int/ITU-T/studygroups/com17/index.asp

13-я Исследовательская комиссия МСЭ-Т (Будущие сети) Вопрос 13: http://www.itu.int/ITU-T/studygroups/com13/index.asp

Проект Liberty Alliance: http://www.projectliberty.org/

Легкая идентичность: http://lid.netmesh.org/wiki/Main_Page

Консорциум MODINIS-IDM: http://www.egov-goodpractice.org и https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

Схемы национальных карт идентичности: например http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/
http://en.wikipedia.org/wiki/Identity_document

OASIS (Организация по разработке стандартов улучшения структурированной информации): http://www.oasis-open.org/home/index.php

ОЭСР (Организация экономического сотрудничества и развития) Семинар по управлению цифровой идентичностью в Тронгейме, Норвегия 8-9 мая 2007 года: http://www.oecd.org/sti/security-privacy/idm.

ОМА (Открытое сообщество производителей мобильной связи): http://www.openmobilealliance.org/

Межправительственная рабочая группа открытого состава: http://www.opengroup.org

OSIS (Система идентичности с открытым исходным кодом): http://osis.netmesh.org/wiki/Main_Page

PAMPAS (Подготовка в ЕС улучшенной конфиденциальности и безопасности в подвижной связи (PAMPAS): http://www.pampas.eu.org/

PERMIS (Инициатива информационного общества ЕС по стандартизации (ISIS) PrivilEge и ее роль

Prime (ЕС управление конфиденциальностью и идентичностью для Европы): https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

W3C (Консорциум World Wide Web): http://www.w3.org/

Yadis: http://yadis.org/wiki/Main_Page

Приложение C

Гиперссылки и справочные документы

Настоящий список справочных материалов будет регулярно обновляться, с учетом результатов реализации Глобальной программы кибербезопасности МСЭ и результатов проекта, реализующего Резолюцию 45 (WTDC-06), работ, выполненных 17-й Исследовательской комиссией МСЭ-Т (Ведущей Исследовательской комиссией МСЭ-Т по кибербезопасности), соответствующих Резолюций ВАСЭ, результатов работ по направлению деятельности С5 ВВУИО по кибербезопасности и результатов работы по соответствующим Резолюциям PP-06 (например, Резолюциям 130, 131 и 149).

ЧАСТЬ I: Разработка и достижение согласованности в отношении национальной стратегии кибербезопасности

I.C.1 Повышение осведомленности (I.B.1, I.B.2)

Международные

- Резолюция 55/63 ГА ООН по "Противодействию преступного злоумышленного использования информационных технологий": http://www.un.org/Depts/dhl/resguide/r55.htm
- Резолюция 56/121 ГА ООН по "Противодействию преступного злоумышленного использования информационных технологий": http://www.un.org/Depts/dhl/resguide/r56.htm
- Резолюция 57/239 ГА ООН по "Созданию глобальной культуры кибербезопасности": http://www.un.org/Depts/dhl/resguide/r57.htm
- Резолюция 58/199 ГА ООН по "Созданию глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур ": http://www.un.org/Depts/dhl/resguide/r58.htm
- Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО), Женевская декларация принципов и План действий, а также Тунисское обязательство и Программа для информационного общества: http://www.itu.int/WSIS/index.html
- Рекомендации ОЭСР по безопасности информационных систем и сетей: К культуре безопасности (2005):http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
- Международный справочник по CIIP 2006 (том 1): http://www.isn.ethz.ch/pubs/ph/details.cfm?id=250
- Ресурсы МСЭ, связанные с кибербезопасностью: http://www.itu.int/cybersecurity/
- Глобальная программа кибербезопасности МСЭ: http://www.itu.int/cybersecurity/gca/
- Шлюз кибербезопасности МСЭ: http://www.itu.int/cybersecurity/gateway/
- Веб-страница Бюро развития МСЭ по кибербезопасности: http://www.itu.int/ITU-D/cyb/
- Инициатива МСЭ "Защита ребенка в онлайновой среде" и соответствующие руководящие указания: http://www.itu.int/cop/

I.C.2 Национальные, региональные и международные стратегии (I.B.2, I.B.3, I.B. 4, I.B.5, I.B.7)

Международные

- Инструментарий МСЭ по национальной кибербезопасности/самостоятельной оценке CIIP: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

- Общие национальные основы защиты важнейшей информационной инфраструктуры (CIIP), разработанные МСЭ и ETH в Цюрихе: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf
- Сектор развития электросвязи МСЭ, Вопрос 22/1для исследовательской комиссии: Обеспечение защиты информации и сети связи: Передовой опыт разработки культуры кибербезопасности: http://www.itu.int/ITU-D/study_groups/SGP_2006-2010/documents/DEFQUEST-SG1/DEFQUEST-Q22-1-E.pdf
- Глобальная программа кибербезопасности МСЭ: http://www.itu.int/cybersecurity/gca/
- Руководство МСЭ по кибербезопасности для развивающихся стран, пересм. 2009 г.: http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf
- Резолюция 45 ВКРЭ МСЭ: Механизмы совершенствования сотрудничества в области кибербезопасности, включая борьбу со спамом (Доха, 2006 г.): http://www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf
- Сектор стандартизации электросвязи МСЭ, 17-я Исследовательская комиссия, Вопрос 4, Справочник – Каталог утвержденных Рекомендаций МСЭ-Т, относящихся к безопасности электросвязи: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090003MSWE.doc
- Сектор стандартизации электросвязи МСЭ, 17-я Исследовательская комиссия, Вопрос 4 – Безопасность в области электросвязи и информационных технологий: http://www.itu.int/pub/T-HDB-SEC.03-2006/en/
- Исследование БРЭ МСЭ по финансовым аспектам безопасности сети. Вредоносные программы и спам: http://www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf
- Рекомендации ОЭСР по безопасности информационных систем и сетей: К культуре безопасности: http://www.oecd.org/document/42/0,3343,en_21571361_36139259_15582250_1_1_1_1,00.html
- План ОЭСР по реализации скоординированных национальных правил онлайновой безопасности: http://www.oecd.org/dataoecd/23/11/31670189.pdf
- Отчет Всемирного банка "Кибербезопасность: новая модель защиты сети": http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2006/12/12/000020953_20061212113151/Rendered/PDF/381170CyberSec1uly0250200601PUBLIC1.pdf
- Ассоциация информационных технологий США (ITAA) Публикация по информационной безопасности: http://www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf

Региональные

- Рабочая группа APEC по электросвязи и информации – Стратегия APEC по кибербезопасности (2002 г.): http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf
- Синяя книга CITEL: Правила электросвязи для Америки (2005 г.) разделы 8.4-8.5: http://www.citel.oas.org/publications/azul-fin-r1c1_i.pdf
- Резолюция Советы Европейского Союза: Стратегия безопасного информационного общества – Диалог, партнерство и расширение полномочий (2007 г.): http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf
- Дохинская декларация по кибербезопасности (2008 г.): http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf
- Европейский союз по связи "Стратегия безопасного информационного общества" (2006 г.): http://ec.europa.eu/information_society/doc/com2006251.pdf

- Программа Европейского союза за более безопасный интернет: http://europa.eu.int/information_society/activities/sip/index_en.htm
- Европейское агентство безопасности сетей и информации (ENISA) Исследование по "Безопасности экономики и внутреннего рынка " (2008 г.): http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm
- Межамериканская стратегия OAS по борьбе с угрозами кибербезопасности (2004 г.): http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

Национальные

- Австралийская программа по моделированию и анализу защиты важнейшей инфраструктуры (CIPMA): http://www.csiro.au/partnerships/CIPMA.html
- Международный справочник CIIP "Кризис и сетевые риски" (CRN): Исследование и анализ национальных правил защиты: http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250
- Национальный план Германии по защите информационной инфраструктуры: http://www.en.bmi.bund.de/cln_028/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf
- Национальная стратегия Японии по информационной безопасности (предварительный перевод): http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf
- Реализация национальных стратегий 11-ю членами ОЭСР: http://www.oecd.org/document/63/0,2340,en_21571361_36139259_36306559_1_1_1_1,00.html
- Цифровая стратегия Новой Зеландии: http://www.digitalstrategy.govt.nz
- Главный план Сингапура по безопасности инфокоммуникаций: http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20080417090044/MR17Apr08MP2.pdf
- Стратегия Сингапура по обеспечению безопасности киберпространства: http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21
- Центр по защите национальной инфраструктуры (CPNI) Соединенного Королевства: http://www.cpni.gov.uk/
- Национальная стратегия США по безопасности киберпространства: http://www.whitehouse.gov/

I.C.3 Разработка и достижение согласованности (I.B.5, I.B.7, I.B.8)

- Задачи управления для информационной технологии и технологий, связанных с ней (COBIT) 4.1: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981 (аннотация – бесплатно; для загрузки полной версии требуется регистрация)
- Библиотека по инфраструктуре информационных технологий (ITIL) Управление безопасностью: http://www.itil-itsm-world.com/ (требуется оплата)
- Международная организация по стандартизации/Международная электротехническая комиссия (ИСО/МЭК), серия 27000, Информационные технологии – Методы безопасности – Системы управления информационной безопасностью: http://www.iso27001security.com/index.html
- ИСО/МЭК 13335, Информационные технологии – Методы безопасности – Управление безопасностью информационных технологий и технологий электросвязи – Часть 1: Концепции и модели управления безопасностью информационных технологий и технологий электросвязи:

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066
(требуется оплата)

- ИСО/МЭК 17799, 2005 Информационные технологии – Методы безопасности – Правила и опыт управления информационной безопасностью: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612
(требуется оплата)
- ИСО/МЭК 21827, Техника безопасности систем – Модель развития возможностей (SSE-CMM®): http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34731
(требуется оплата)
- Исследование БРЭ МСЭ финансовых аспектов безопасности сети: Вредоносные программы и спам: http://www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf
- Резолюция 50 (Пересм. Йоханнесбург, 2008 г.) ВАСЭ МСЭ: Кибербезопасность: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf
- Резолюция 52 (Пересм. Йоханнесбург, 2008 г.) ВАСЭ МСЭ: Противодействие распространению спама и борьба со спамом: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf
- Резолюция 58 (Йоханнесбург, 2008 г.) ВАСЭ МСЭ: Поощрение создания национальных групп реагирования на компьютерные инциденты, в частности для развивающихся стран: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf
- Специальная публикация NIST (SP) 800-12, Введение в компьютерную безопасность: Справочник NIST (февраль 1996 г.): http://csrc.nist.gov/publications/nistpubs/800-12/
- NIST SP 800-30, Руководство по управлению рисками для систем информационных технологий (июль 2002 г.): http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- NIST SP 800-53, Рекомендованные методы управления безопасностью для федеральных информационных систем (декабрь 2007 г.): http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
- Проект специальной публикации NIST 800-53A, Руководство по оценке методов управления безопасностью для федеральных информационных систем (декабрь 2007 г.): http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-A
- NIST SP 800-50 Создание осведомленности о безопасности информационных технологий и программа обучения (октябрь 2003 г.): http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
- NIST SP 800-30 Руководство по управлению рисками в системах информационных технологий, (июль 2002 г.): http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Угрозы, опасные для эксплуатации, оценка активов и уязвимости SM (OCTAVESM): http://www.cert.org/octave/

I.C.4 Контактные пункты международной помощи (I.B.6)

- Рабочая группа по антифишингу (APWG): http://www.antiphishing.org
- Форум групп реагирования на инциденты в области безопасности (FIRST): http://www.first.org
- Институт инженеров по электротехнике и электронике: http://www.ieee.org
- Рабочая группа по инженерным проблемам интернета: http://www.ietf.org
- Рабочая группа противодействия злонамеренному использованию служб передачи сообщений: http://www.maawg.org
- Всемирный альянс служб информационных технологий: http://www.witsa.org
- Консорциум World Wide Web: http://www.w3c.org

ЧАСТЬ II: Налаживание сотрудничества между государством и промышленностью

II.C.1 Структуры сотрудничества государства с промышленностью

Международные

- Промышленный альянс кибербезопасности: http://www.csialliance.org/about_csia/index.html
- Антиспамовый инструментарий ОЭСР – Партнерское сотрудничество против спама: http://www.oecd-antispam.org/article.php3?id_article=243
- StopSpamAlliance.org: http://stopspamalliance.org/

Региональные

- Ближний Восток: Отчет о 14-м форуме GCC по вопросам eGovernment и eServices: http://www.zawya.com/Story.cfm/sidZAWYA20080529073202/SecMain/pagHomepage/chnAll%20Regional%20News/obj2A17E941-F5E0-11D4-867D00D0B74A0D7C/

Национальные

- Австралийское партнерство бизнеса государства: Доверенная сеть совместного использования информации для защиты важнейшей инфраструктуры: http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_CriticalInfrastructureProtectionModellingandAnalysis(CIPMA)
- Центры США по совместному использованию и анализу информации (ISAC) и Координационные советы:
  - ISAC для финансовых служб: http://www.fsisac.com/
  - ISAC для сектора электроэнергетики: http://www.esisac.com/
  - ISAC по информационным технологиям: http://www.it-isac.org
  - ISAC по электросвязи: http://www.ncs.gov/ncc/
  - Совет по надежности и взаимодействию сети (NRIC): http://www.nric.org/
  - Национальный консультативный комитет по безопасности и электросвязи (NSTAC): http://www.ncs.gov/nstac/nstac.html
- Содружество правительства и промышленности США по вопросам стандартизации: Американский национальный институт стандартов-Бюро стандартов национальной безопасности: http://www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3
- Публикация по информационной безопасности Американской ассоциации по информационным технологиям США: http://www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf
- Координационный совет IT сектора США (SCC): http://www.it-scc.org
- Партнерство США по национальной кибербезопасности: http://www.cyberpartnership.org/
- Отчет рабочей группы Совета по обеспечению безопасности национальной информации (NIAC) по модели партнерства в секторе промышленности: http://itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf
- План США по защите национальной инфраструктуры: http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm
- Планы США для конкретных секторов: http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- Планы США для IT сектора: http://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf
- Национальная администрация США по электросвязи и информации: http://www.ntia.doc.gov/

II.C.2 Совместное использование информации по кибербезопасности

Международные

- Рабочая группа противодействия злонамеренному использованию служб передачи сообщений: http://www.maawg.org

Национальные

- NIST США, Центр по компьютерной безопасности и исследованиям: http://csrc.nist.gov/
- US-CERT США Национальная система оповещения о киберугрозах: http://www.us-cert.gov/cas/

II.C.3 Повышение осведомленности и программа помощи: Инструментарий для правительств и промышленности

Международные

- Программа повышения осведомленности о безопасности: http://www.gideonrasmussen.com/article-01.html
- Центр ресурсов безопасности интернета и публикации по безопасности предприятия: http://www.cisecurity.org/resources.html
- Корпоративные стратегии по осведомленности о безопасности: http://articles.techrepublic.com.com/5100-10878_11-5193710.html
- Руководство по общим принципам кибербезопасности для малых предприятий: http://www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm
- EDUCAUSE Ресурсы повышения осведомленности о безопасности для правительства и промышленности: http://www.educause.edu/Security%20Task%20Force/CybersecurityAwarenessResource/BrowseSecurityAwarenessResourc/8770?time=1215527945
- ENISA Инициативы осведомленности об информационной безопасности (имеются на нескольких языках): http://www.enisa.europa.eu/Pages/05_01.htm
- Методы Интерпола по безопасности IT и предотвращению преступлений (для предотвращения преступлений в компаниях): http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp
- Проверочный лист Интерпола по IT преступлениям в компаниях: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp
- Постеры осведомленности о безопасности NoticeBored: http://www.noticebored.com/html/posters.html
- Антиспамовый инструментарий ОЭСР – Обучение и повышение осведомленности: http://www.oecd-antispam.org/article.php3?id_article=242
- Ресурсы политик безопасности SANS: http://www.sans.org/resources/policies/
- Инструментарий осведомленности о безопасности – Сайт информационных войн: http://www.iwar.org.uk/comsec/resources/sa-tools/
- Национальное партнерство США по кибербезопасности – Осведомленность для малых предприятий и центр ресурсов для малых предприятий: http://www.cyberpartnership.org/init-aware.html

Национальные

- Федеральная торговая комиссия США: http://www.ftc.gov/infosecurity
- Программа повышения осведомленности и обучения безопасности NIST 800-50: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

ЧАСТЬ III: Предотвращение киберпреступности/правовые основы и охрана правопорядка

Международные

- Совет Европы: Конвенция о киберпреступности (2001 г.): http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- Принципы G8 по высокотехнологичным преступлениям: http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html
- Справочный материал МСЭ, относящийся к гармонизации национальных правовых подходов, международной правовой координации и охраны правопорядка: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- Регуляторный инструментарий МСЭ/InfoDev для ИКТ: http://www.ictregulationtoolkit.org/
- Публикация МСЭ "Понимание киберпреступности": Руководство для развивающихся стран: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html
- Комплект материалов МСЭ по законодательству в области киберпреступности: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html
- Ресурсы Интерпола по преступлениям в сфере информационных технологий: http://www.interpol.com/Public/TechnologyCrime/
- Антиспамовые регуляторные подходы ОЭСР: http://www.oecd-antispam.org/article.php3?id_article=1
- Антиспамовый инструментарий ОЭСР: http://www.oecd-antispam.org/article.php3?id_article=265
- Резолюция 55/63 ГА ООН по "Противодействию преступного злоумышленного использования информационных технологий": http://www.un.org/Depts/dhl/resguide/r55.htm
- Резолюция 56/121 ГА ООН по "Противодействию преступного злоумышленного использования информационных технологий": http://www.un.org/Depts/dhl/resguide/r56.htm
- Ресурсы Межрегионального научно-исследовательского института ООН по вопросам преступности и правосудия (UNICRI) для повышения осведомленности и создания новых партнерств для борьбы с киберпреступностью: http://www.unicri.it/
- Модели законов UNCITRAL по электронной торговле и электронным подписям: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
- Ресурсы Управления ООН по наркотикам и преступности: http://www.unodc.org/

Региональные

- APEC: Документы, презентации и правительственные заявления по киберпреступности: http://www.apectelwg.org/
- Каирская Декларация конференции по киберпреступности: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf
- Модельные законы Содружества по компьютерным преступлениям и преступлениям, связанным с компьютерами: http://www.thecommonwealth.org/Internal/38061/documents/
- Совет Европы: Конвенция по киберпреступности (2001 г.): http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- OAS: Межамериканский общий портал по киберпреступности: http://www.oas.org/juridico/english/cyber.htm

Национальные

- CERT/CC: Как ФБР расследует компьютерные преступления: http://www.cert.org/tech_tips/FBI_investigates_crime.html

- Cybercrimelaw: Всемирный обзор законодательства по киберпреступности: http://www.cybercrimelaw.net/index.html
- Совет Европы: Обзор законодательств по киберпреступности в разных странах: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/Legprofiles.asp#TopOfPage
- Microsoft: "Анализ Азиатско-тихоокеанского законодательства: Существующие и незавершенные законы по онлайновой безопасности и киберпреступности": http://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf
- Антиспамовые законы государств – членов ОЭСР: http://www.oecd-antispam.org/countrylaws.php3
- ООН "Модели законодательства для киберпространства в странах – членах Экономической и социальной комиссии для Западной Азии (ESCWA)": http://www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf
- Веб-сайт по компьютерным преступлениям и интеллектуальной собственности Министерства юстиции США (USDOJ: http://www.cybercrime.gov
- Министерства юстиции США (USDOJ) Справочник по разработке компьютерных преступлений (Глава 1 – Закон о компьютерном мошенничестве и злонамеренном использовании): http://www.cybercrime.gov/ccmanual/
- Секретная служба США – Передовой опыт сбора электронных доказательств: http://www.forwardedge2.com/pdf/bestPractices.pdf

ЧАСТЬ IV: Создание национального потенциала по управлению инцидентами: наблюдение, предупреждение, реагирование и восстановление

IV.C.1 Национальный план реагирования и национальные CIRT

Международные

- Координационный центр CERT (CERT/CC) в Университете Карнеги-Меллона: http://www.cert.org/csirts/
- CERT/CC: Список действий для разработки CSIRT: http://www.cert.org/csirts/action_list.html
- CERT/CC: Создание CSIRT: Процедуры начала работ: http://www.cert.org/csirts/Creating-A-CSIRT.html
- CERT/CC: Определение процедур управления инцидентами для CSIRT: Продолжение работ: http://www.cert.org/archive/pdf/04tr015.pdf
- CERT/CC: CSIRT Часто задаваемые вопросы: http://www.cert.org/csirts/csirt_faq.html
- CERT/CC: Справочник для CSIRT: http://www.cert.org/archive/pdf/csirt-handbook.pdf
- CERT/CC: Метрики для измерения возможностей управления инцидентами. Версия 0.1: http://www.cert.org/archive/pdf/07tr008.pdf
- CERT/CC: Организационные модели для CSIRT: http://www.cert.org/archive/pdf/03hb001.pdf
- /CC: Услуги CSIRT: http://www.cert.org/csirts/services.html
- CERT/CC: Найм персонала для вашей CSIRT – Какие основные навыки требуются?: http://www.cert.org/csirts/csirt-staffing.html
- CERT/CC: Состояние работ в CSIRT: http://www.cert.org/archive/pdf/03tr001.pdf
- CERT/CC: Этапы создания национальных CSIRT: http://www.cert.org/archive/pdf/NationalCSIRTs.pdf
- CERT/CC Виртуальная обучающая среда (VTE): http://www.vte.cert.org/

- ENISA: Пошаговый подход к задаче организации CSIRT: http://www.enisa.europa.eu/pages/05_01.htm
- Сотрудничество МСЭ-ИМПАКТ и соответствующие ресурсы: http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html
- GOVCERT.nl: CSIRT в коробке – Информация о создании CSIRT: http://www.govcert.nl/render.html?it=69
- CPNI Соединенного Королевства: Инструментарий пункта оповещения, консультаций и сбора отчетов (WARP): http://www.warp.gov.uk/

Региональные

- Азиатско-Тихоокеанская CERT: http://www.apcert.org/index.html
- Сетевые ресурсы европейской CSIRT: http://www.ecsirt.net/
- Группа CERT Европейского союза (EGC): http://www.egc-group.org/

Национальные

- Австралия: AusCERT: http://www.auscert.org.au
- Австрия: CERT.at: http://www.cert.at
- Бразилия: CERT.br: http://www.cert.br/
- Чили: CLCERT: http://www.clcert.cl/
- Китай: CNCERT/CC: http://www.cert.org.cn/
- Финляндия: CERT-FI: http://www.cert.fi
- Венгрия: CERT-Hungary: http://www.cert-hungary.hu
- Индия: CERT-In: http://www.cert-in.org.in
- Италия: CERT-IT: http://security.dico.unimi.it/
- Япония: JPCERT/CC: http://www.jpcert.or.jp/
- Корея: KrCERT/CC: http://www.krcert.or.kr/
- Малайзия: MyCERT: http://www.cybersecurity.org.my
- Нидерланды: http://www.csirt.dk/
- Польша: CERT POLSKA: http://www.cert.pl/
- Словения: SI-CERT: http://www.arnes.si/en/si-cert/
- Сингапур: SingCERT: http://www.singcert.org.sg/
- Швеция: SITIC: http://www.sitic.se
- Швейцария: MELANI: http://www.melani.admin.ch
- Таиланд: ThaiCERT: http://www.thaicert.nectec.or.th/
- Тунис: CERT-TCC: http://www.ansi.tn/en/about_cert-tcc.htm
- Катар: http://www.qcert.org
- Объединенные Арабские Эмираты: http://aecert.ae/
- Национальный план реагирования США: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml
- Соединенные штаты Америки US-CERT: http://www.us-cert.gov/
- И веб-сайты других национальных CERT/CSIRT

IV.C.2 Сотрудничество и обмен информацией

Международные

- CERT/CC: Уязвимости безопасности и способы их устранения: http://www.cert.org/nav/index_red.html
- Центр анализа и синтеза информации для инструментов работы с инцидентами (CHIHT): http://chiht.dfn-cert.de/
- Ресурсы форума групп реагирования на инциденты и безопасности (FIRST): http://www.first.org/
- Ресурсы службы поддержки безопасности ISP: http://www.donelan.com/ispsupport.html
- Шлюз кибербезопасности МСЭ: Базовый материал по вопросам наблюдения, предупреждения и реагирования на инциденты: http://www.itu.int/cybersecurity/gateway/watch_warning.html
- Система оповещения малых предприятий и граждан ITsafe: http://www.itsafe.gov.uk/
- ОЭСР: Антиспамовый инструментарий: http://www.oecd-antispam.org/article.php3?id_article=265

Региональные

- Трансъевропейская ассоциация исследования и изучения сетей (TERENA): http://www.terena.org/

Национальные

- Нидерланды: Голландская национальная служба оповещения: http://www.waarschuwingsdienst.nl/render.html?cid=106
- CPNI Соединенного Королевства: Инструментарий пункта оповещения, консультаций и сбора отчетов (WARP): http://www.warp.gov.uk/
- IT-ISAC Соединенных штатов Америки: https://www.it-isac.org/
- Координационный совет сектора IT США (ISCC): Информационные технологии: Специальный план сектора по важнейшей инфраструктуре и ключевым ресурсам: http://www.it-scc.org/documents/itscc/Information_Technology_SSP_2007.pdf
- Национальный институт США по стандартам и технологии (NIST): http://csrc.nist.gov/

IV.C.3 Информация об уязвимости/Инструменты и методы

- Встроена безопасность – Библиотека информации о надежности программ и безопасности, полезная при создании систем безопасности: https://buildsecurityin.us-cert.gov/daisy/bsi/home.html
- Перечень общих уязвимостей и рисков (CVE): http://www.cve.mitre.org/about/
- Открытый язык оценки уязвимости (OVAL): http://oval.mitre.org/
- США – Национальная база данных уязвимостей программного обеспечения (NVD): http://nvd.nist.gov/nvd.cfm

ЧАСТЬ V: Содействие развитию национальной культуры кибербезопасности

V.C.1 Правительственные системы и сети (V.B.1, V.B.2, V.B.7)

Международные

- Направление действия С5 ВВУИО, План действий: http://www.itu.int/wsis/implementation/index.html
- Глобальный план действий по кибербезопасности МСЭ: http://www.itu.int/osg/csd/cybersecurity/gca/

- Тематическое собрание МСЭ ВВУИО по противодействию спаму: http://www.itu.int/osg/spu/spam/meeting7-9-04/index.html
- Направление действия С5 ВВУИО, Отчет председателя первого собрания: http://www.itu.int/osg/spu/cybersecurity/2006/chairmansreport.pdf
- Направление действия С5 ВВУИО, План действия второго собрания: http://www.itu.int/wsis/docs/geneva/official/poa.html
- Повестка дня второго собрания со ссылками на презентации: http://www.itu.int/osg/csd/cybersecurity/ВВУИО/meetingAgenda.html
- Направление действия С5 ВВУИО, Отчет о третьем собрании: http://www.itu.int/osg/csd/cybersecurity/ВВУИО/3rd_meeting_docs/ВВУИО_Action_Line_C5_Meeting_Report_June_2008.pdf
- Повестка дня Третьего собрания со ссылками на презентации: http://www.itu.int/osg/csd/cybersecurity/ВВУИО/agenda-3_new.html
- Microsoft: Конфиденциальность вычислений, безопасность интернета и информация о безопасности для разработчиков правил всего мира: http://www.microsoft.com/mscorp/twc/policymakers_us.mspx
- Портал ОЭСР по культуре безопасности с ресурсами: http://www.oecd.org/sti/cultureofsecurity
- ОЭСР "Руководство по системам защиты информации и сетей. К культуре безопасности" (2002 г.): http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html
- ОЭСР: "Руководство по защите конфиденциальности и трансграничным потокам персональных данных" (1980 г.): http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html
- Отчет ОЭСР "Продвижению культуры для информационных систем и сетей в странах ОЭСР" (2005 г.): http://www.oecd.org/dataoecd/16/27/35884541.pdf
- Справочник Всемирного банка по безопасности информационных технологий – Информационная безопасность и политика правительства: http://www.infodev-security.net/handbook/part4.pdf
- Резолюция UNGA 57/239 (Приложения a и b.): http://www.un.org/Depts/dhl/resguide/r57.htm

Региональные

- ENISA: "Инициативы по осведомленности об информационной безопасности: Сегодняшний опыт и меры успеха" (2007 г.): http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf
- ENISA: "Руководство пользователя: Как повысить осведомленность об информационной безопасности" (2006 г.): http://www.enisa.europa.eu/doc/pdf/deliverables enisa_a_users_guide_how_to_raise_IS_awareness.pdf
- Европейский источник информации о безопасности интернета (InSafe): http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- OAS: Межамериканская стратегия по противостоянию угрозам кибербезопасности: Многомерный и междисциплинарный подход к созданию культуры кибербезопасности (в частности, приложения) (2004 г.): http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

Национальные

- Бразилия: ресурсы Antispam.br: http://antispam.br/
- Бразилия: руководящие указания по безопасному использованию интернета Руководящего комитета по вопросам интернета Бразилии – CGI.br: http://cartilha.cert.br/
- Инициативы ОЭСР по продвижению культуры безопасности (по странам): http://www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html
- Сайт CERT США: http://www.us-cert.gov/

- План США по защите важнейшей национальной инфраструктуры DHS R&D: http://www.dhs.gov/xres/programs/gc_1159207732327.shtm
- Опыт Федерального агентства безопасности США: http://csrc.nist.gov/fasp/
- Федеральные правила закупок США (FAR), части 1,2,7,11 и 39: http://www.acqnet.gov/FAR/
- Федеральный план США по кибербезопасности и защите информации R&D: http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf
- Консультативный совет США по информационной безопасности конфиденциальности: http://csrc.nist.gov/ispab/
- Директива Президента США по национальной безопасности /HSPD-7, "Определение важнейшей инфраструктуры, приоритеты и защита": http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
- Центр США по анализу и совместному использованию информации различными штатами: http://www.msisac.org/
- Национальная стратегия США по безопасности в киберпространстве: http://www.whitehouse.gov/pcipb/
- Отчет консультативного комитета по информационным технологиям при президенте США по приоритетам исследований проблем безопасности киберпространства: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

V.C.2 Организации промышленности и частных лиц (V.B.3, V.B.5, V.B.7)

- Движение за безопасный интернет Бразилии: http://www.internetsegura.org/
- Центр безопасности Cisco (Раздел о передовом опыте): http://tools.cisco.com/security/center/home.x
- Доверенные вычисления Microsoft: http://www.microsoft.com/mscorp/twc/default.mspx
- Обучающие материалы NIATEC: http://niatec.info/index.aspx?page=105
- Справочник Всемирного банка по безопасности информационных технологий – Безопасность для организаций: http://www.infodev-security.net/handbook/part3.pdf
- Постеры и информационные плакаты CERT МСША для рабочих мест: http://www.uscert.gov/reading_room/distributable.html
- Работы DHS/промышленности США "Кибершторм": http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm

V.C.3 Люди и гражданское общество (V.B.4, V.B.6, V.B.7)

- Бразилия: SaferNet Brazil: http://www.safernet.org.br/site/
- Будь в безопасности он-лайн (SUSI – Безопасное использование услуг интернета): http://www.besafeonline.org/
- Советы по безопасности CASEScontact: http://casescontact.org/tips_list.php
- Childnet – Международные ресурсы для детей: http://www.childnet-int.org
- Инициатива Кибермир: http://www.cyberpeaceinitiative.org/
- CyberTipline: Подростки учатся, как оставаться в безопасности онлайн: http://tcs.cybertipline.com/
- Ресурсы Безопасной зоны интернета для детей и родителей: http://www.internetsafetyzone.co.uk/
- Конфиденциальный опросный лист по IT преступлениям: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/privateChecklist.asp
- Инициатива МСЭ "Защита ребенка в онлайновой среде" и соответствующие руководящие указания: http://www.itu.int/cop/

- Инструментарий GetNetWise для семей: http://kids.getnetwise.org/tools/
- OnGuard Online – советы по защите от мошенничества: http://onguardonline.gov/index.html
- MakeItSecure – информация о часто встречающихся опасностях интернета: http://www.makeitsecure.org/en/index.html
- Инициатива Малайзии eSecurity: http://www.esecurity.org.my/
- NetSmartz: ресурсы для родителей и воспитателей: http://www.netsmartz.org/netparents.htm
- Netsafe Новой Зеландии: http://www.netsafe.org.nz
- Горячая линия SafeLine для сообщений о незаконном контенте: http://www.safeline.gr/
- Мультфильмы по безопасности: http://www.securitycartoon.com/
- Будь в безопасности он-лайн: http://www.staysafeonline.info/
- WiredSafety.org: http://www.wiredsafety.org/
- Справочник Всемирного банка по безопасности информационных технологий – Безопасность для граждан: http://www.infodev-security.net/handbook/part2.pdf
- Ресурсы Центра Соединенного Королевства по эксплуатации детей и защите в режиме он-лайн: http://www.ceop.gov.uk/
- Сайт "Будь в безопасности он-лайн Соединенного Королевства": http://www.getsafeonline.org/
- CERT США для пользователей-нетехнарей: http://www.us-cert.gov/nav/nt01/

И другие международные, региональные и национальные инициативы по повышению осведомленности конечных пользователей.

Отпечатано в Швейцарии
Женева, 2010 г.

Фотографии представлены: МСЭ Библиотека фотографий