Академия ИКТ для лидеров государственного управления

Модуль 6

Обеспечение информационно-сетевой безопасности и неприкосновенности частной жизни

Корейское агентство по информационной безопасности

APCICT

АЗИАТСКО-ТИХООКЕАНСКИЙ УЧЕБНЫЙ ЦЕНТР ПО ИНФОРМАЦИОННЫМ И КОММУНИКАЦИОННЫМ ТЕХНОЛОГИЯМ ДЛЯ РАЗВИТИЯ

УДК 004
ББК 32.88
М 74

Серия модулей Академии ИКТ для лидеров государственного управления

М 74 Модуль 6: Обеспечение информационно-сетевой безопасности и неприкосновенности частной жизни. - Б.: 2009. - 124 с.

ISBN 978-9967-25-635-4
ISBN 978-9967-25-638-5 (общ.)

United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT)
Bonbudong, 3rd Floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu-gu, Incheon City
Republic of Korea

Telephone: +82 32 245 1700-02
Fax: +82 32 245 7712
E-mail: info@unapcict.org
http://www.unapcict.org

M 2303010000-09
ISBN 978-9967-25-635-4
ISBN 978-9967-25-638-5 (общ.)

УДК 004
ББК 32.88

ПРЕДИСЛОВИЕ К СЕРИИ МОДУЛЕЙ АКАДЕМИИ ИКТ ДЛЯ ЛИДЕРОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

21 век характеризуется растущей взаимозависимостью людей в глобализирующемся мире. Это мир, где открываются возможности для миллионов людей с помощью новых технологий, расширенного доступа к необходимой информации и знаниям, которые могут существенно улучшить жизнь людей и способствовать сокращению бедности. Но это возможно лишь в том случае, если растущая взаимозависимость сопровождается обменом ценностей, приверженностью и солидарностью для всеобъемлющего и устойчивого развития, где прогресс служит всем народам.

Что касается развития информационно-коммуникационных технологий (ИКТ), то в последние годы Азия и Тихий океан были «регионом превосходной степени». По данным Международного союза электросвязи в регионе проживают более 2 млрд. абонентов фиксированной связи и 1,4 млрд. подписчиков мобильной связи. К середине 2008 г. только в Китае и Индии насчитывалось четверть всех мобильных телефонов в мире. На Азиатско-Тихоокеанский регион также приходится 40 процентов мировых Интернет-пользователей и самый большой в мире рынок широкополосного Интернета с долей в 39 процентов от общемирового объема.

На фоне быстрого технического прогресса многие задались вопросом о возможности устранения цифрового неравенства. К сожалению, ответ на данный вопрос – пока «еще нет». Даже спустя пять лет после Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), состоявшейся в Женеве в 2003 году, и, несмотря на все впечатляющие технологические достижения и обязательства ключевых игроков в регионе, основные средства связи до сих пор находятся вне доступа подавляющего большинства людей, особенно бедных.

Более чем в 25 странах региона, главным образом, небольших островных развивающихся государствах и развивающихся странах, не имеющих выхода к морю, имеются менее 10 пользователей Интернета на 100 человек, и эти пользователи, в основном, сосредоточены в крупных городах, в то время как некоторые развитые страны в регионе имеют соотношение более 80 пользователей Интернета на 100 человек. Различие в обеспечении широкополосным Интернетом между развитыми и развивающимися странами еще более впечатляющее.

В целях преодоления цифрового неравенства и реализации потенциала ИКТ для всеобъемлющего социально-экономического развития в регионе разработчикам политики в развивающихся странах необходимо будет установить приоритеты, принять политику, разработать нормативно-правовую базу, выделить финансовые средства, а также содействовать налаживанию партнерских связей, способствующих развитию отрасли ИКТ-индустрии и навыков в области ИКТ среди своих граждан.

В Плане действий ВВУИО говорится: «… каждый человек должен иметь возможность приобрести необходимые навыки и знания для того, чтобы понять, участвовать и использовать преимущества информационного общества и экономики знаний». С этой целью в рамках Плана действий содержится призыв к международному и региональному сотрудничеству в области наращивания потенциала с упором на создание критической массы квалифицированных специалистов и экспертов в области ИКТ.

Именно в ответ на этот призыв Азиатско-Тихоокеанский учебный центр по информационным и коммуникационным технологиям для развития (АТУЦ ИКТР) разработал данную всеобъемлющую учебную программу по обучению ИКТ для развития – Академия ИКТ для лидеров государственного управления – состоящей в настоящее время из восьми самостоятельных, но взаимосвязанных модулей, направленных на распространение основных знаний и опыта, которые помогут разработчикам политики планировать и осуществлять инициативы в области ИКТ более эффективно.

АТУЦ ИКТР является одним из пяти региональных институтов Экономической и социальной комиссии для Азии и Тихого океана (ЭСКАТО). ЭСКАТО содействует устойчивому и всеобъемлющему социально-экономическому развитию в Азии и Тихоокеанском регионе на основе анализа, нормативной работы, наращивания потенциала, регионального сотрудничества и обмена знаниями. В партнерстве с другими агентствами ООН, международными организациями, национальными партнерами и заинтересованными сторонами ЭСКАТО через АТУЦ ИКТР обязуется оказывать поддержку использованию, усовершенствованию и переводу данных модулей Академии в разных странах, а также организацию их преподавания на регулярной основе через национальные и региональные семинары для правительственных должностных лиц старшего и среднего уровня, цель которых в том, чтобы возросший потенциал и полученные знания трансформировались в зрелое понимание выгод от ИКТ и конкретные меры в достижении целей в области развития.

Ноэлин Хейзер

Заместитель Генерального секретаря Организации Объединенных Наций
Исполнительный секретарь ЭСКАТО

ПРЕДИСЛОВИЕ

Путешествие в процесс разработки серии модулей Академии ИКТ для лидеров государственного управления было поистине вдохновляющим и поучительным опытом. Оно не только послужило для заполнения пробелов в создании потенциала в области ИКТ, но также проложило новый путь для разработки программ учебных курсов – через участие многочисленных людей и чувства причастности к процессу.

Академия является флагманом программ АТУЦ ИКТР, разработанного на основе активных исследований и анализа сильных и слабых сторон существующих учебных материалов, а также процесса рецензирования среди ведущих экспертов. Во многих регионах прошли обучающие семинары Академии, обеспечивших неоценимую возможность для обмена опытом и знаниями между участниками из разных стран, процесс, который сделал выпускников Академии ведущими игроками по подгонке и формированию модулей.

Начало преподавания первых восьми модулей Академии на национальном уровне знаменует собой зарождение жизнетворного процесса укрепления существующих партнерских отношений и построение новых для усиления потенциала в области разработки политики ИКТ для развития (ИКТР) по всему региону. АТУЦ ИКТР выражает приверженность к оказанию технической поддержки в начале деятельности национальных Академий, как своего ключевого подхода в обеспечении процесса охвата Академией всех разработчиков политики. Центр тесно сотрудничает с рядом региональных и национальных учебных заведений, которые уже имеют непосредственную связь с центральными, государственными и местными органами управления по усилению их потенциала в области ИКТР путем локализации, перевода и обучения модулей Академии, которые уделяют особое внимание национальным потребностям и приоритетам. Также существуют планы по дальнейшему расширению масштаба и охвата существующих модулей и разработке новых.

Кроме того, АТУЦ ИКТР берет на вооружение многоуровневый подход для обеспечения того, что содержание модулей Академии достигнет большей аудитории в регионе. Наряду к непосредственному обучению материалов Академии через региональные и национальные Академии АТУЦ ИКТР учредил Виртуальную Академию АТУЦ ИКТР (APCICT Virtual Academy, AVA), которая является сетевой дистанционной обучающей платформой Академии и предназначена для обеспечения участников возможностью изучать материалы по своему усмотрению. AVA гарантирует, что все модули Академии и сопутствующие материалы, такие как слайды презентаций и тематические исследования легко доступны в сети для загрузки, многократного использования, усовершенствования и локализации, а также она содержит различные функции, в том числе виртуальные лекции, учебные средства для организации процесса обучения и разработки нового содержания, а также сертификации.

Первоначальная серия из восьми модулей и их обучение в рамках региональных, субрегиональных и национальных семинаров Академии было бы невозможно без приверженности делу и инициативного участия многих людей и организаций. Я хотела бы воспользоваться этой возможностью, чтобы отметить усилия и достижения выпускников Академии и наших партнеров из правительственных ведомств, учебных заведений, а также региональных и национальных организаций, принявших участие в семинарах Академии. Они не только внесли ценный вклад в содержание модулей, но, что более важно, они стали сторонниками Академии в своих странах, в результате чего были подписаны соглашения между АТУЦ ИКТР и рядом национальных и региональных учреждений-партнеров в целях усовершенствования и проведения регулярных курсов Академии в странах.

Также я хотела бы добавить особую признательность самоотверженным усилиям многих выдающихся людей, которые сделали данное необычайное путешествие возможным. Это Шахид Акхтар, советник проекта Академии; Патриция Аринто, редактор; Кристина Апикул, выпускающий редактор; все авторы модулей Академии и команда АТУЦ ИКТР.

Для того чтобы ценные знания, изложенные в Академии, резонансно распространялись среди людей во всех уголках Азии и Тихого океана, АТУЦ ИКТР и его партнеры неустанно работали над переводом и локализацией содержания Академии. Именно благодаря этим усилиям мы в настоящее время публикуем русскую версию Академии.

Команда по подготовке русской версии Академии провела много времени, чтобы терминология соответствовала текущему применению в языке, нюансы и тонкости были отражены, а перевод содержания был обоснован. В этом смысле они оказались вторыми авторами модулей Академии. Я хотела бы выразить мою глубокую признательность Национальному центру информационных технологий в Кыргызстане, его сотрудникам за их самоотверженные усилия и приверженность этой инициативе. В частности, я хотела бы отметить выдающуюся работу, проделанную Алмазом Бакеновым, Мунар Усубалиевой, Бэллой Молдобаевой, Андреем Смиренским, Дмитрием Петренко, Аманбеком Бавланкуловым, Эмилем Албановым и Медером Мамутовым.

Я искренне надеюсь, что Академия будет способствовать народам по сокращению нехватки человеческих ресурсов в области ИКТ, устранению барьеров на пути внедрения ИКТ, содействовать применению ИКТ в ускорении социально-экономического развития и достижения Целей развития тысячелетия.

Хеун-Сук Ри

Директор
АТУЦ ИКТР

О СЕРИИ УЧЕБНЫХ МОДУЛЕЙ

В современный «век информации» простой доступ к информации меняет наш образ жизни, работы и развлечений. «Цифровая экономика», также известная как «экономика знаний», «сетевая экономика» или «новая экономика», характеризуется переходом от производства товаров к созданию идей. Это подчеркивает рост, если уже не главенство, роли информационных и коммуникационных технологий (ИКТ) в экономике и в обществе в целом.

Как следствие, правительства во всем мире уделяют все больше внимания на ИКТ в целях развития (ИКТР). Для правительств этих стран ИКТР заключается не только в развитии индустрии ИКТ или сектора экономики, но также и во включении ИКТ в экономику для стимулирования как социального, так и политического роста.

Тем не менее, помимо трудностей, с которыми сталкивается правительство при разработке политики в области ИКТ, существует тот факт, что разработчики политики зачастую не знакомы с технологиями, которые они используют в целях национального развития. Поскольку никто не может управлять тем, с чем не знаком, многие политики уклоняются от разработки политики в области ИКТ. Но предоставление разработки политики в области ИКТ «технарям» также неправильно, поскольку зачастую они не имеют представления о политических последствиях разработки и использования технологий.

Серия модулей Академии ИКТ для лидеров государственного управления была разработана Азиатско-Тихоокеанским учебным центром ООН по информационным и коммуникационным технологиям в целях развития (АТУЦ ИКТР) для:

1. Политиков общенационального и местного уровней управления, ответственных за разработку политики в области ИКТ;

2. Государственных должностных лиц, ответственных за разработку и внедрение приложений на основе ИКТ;

3. Руководителей государственного сектора, стремящихся использовать средства ИКТ для управления проектами.

Серия модулей стремится познакомить с практическими вопросами, связанными с ИКТР, с точки зрения, как политики, так и технологии. Цель состоит не в разработке технического руководства по ИКТ, а скорее в том, чтобы обеспечить хорошее понимание возможностей современных цифровых технологий или в каком направлении они будут развиваться, и что это означает для разработки политических решений. Темы, раскрываемые в модулях, были определены на основе анализа потребностей в обучении и изучения учебных материалов, применяемых в других странах мира.

Данные модули разработаны таким образом, что они могут применяться для самостоятельного изучения отдельными читателями, либо в качестве ресурса в ходе подготовки или программы. Эти модули сами по себе являются автономными, но в то же время связаны между собой, и были предприняты усилия, чтобы связать между собой темы и обсуждения в модулях серии. Долгосрочной целью является объединение модулей в цельный курс, который может пройти соответствующую сертификацию.

В начале каждого модуля излагаются цели и задачи обучения, по которым читатель сможет оценить свои успехи. Содержание модуля разбито на отдельные разделы, включающие тематические исследования и упражнения, помогающие глубже понять ключевые концепции. Упражнения можно выполнять индивидуально и в группах. Для иллюстрации определенных аспектов обсуждения в модуль включены таблицы и рисунки. Также вниманию читателей представлены ссылки на литературные источники и Интернет-ресурсы, чтобы предоставить возможность получения дополнительной информации и знаний.

Применение ИКТР является настолько разнообразным, что некоторые тематические исследования и примеры, рассматриваемые в учебных модулях, могут показаться противоречащими друг другу. Этого следует ожидать, так как это очень новая и сложная дисциплина, и предполагается, что все страны мира должны включиться в процесс изучения возможностей ИКТ в качестве инструмента для развития.

Поддержка серии модулей Академии в печатном формате осуществляется на платформе интерактивного дистанционного обучения в сети – Виртуальной Академией АТУЦ ИКТР (AVA – http://www.unapcict.org/academy) — в которой применяются виртуальные классы, показывающие выступления преподавателей в видео формате и презентации PowerPoint учебных модулей.

Кроме того, АТУЦ ИКТР разработал электронный центр ИКТР для совместной работы (e-Collaborative Hub) (e-Co Hub – http://www.unapcict.org/ecohub), выделенный сетевой ресурс для практиков и политиков в целях повышения их опыта в области обучения и преподавания. E-Co Hub предоставляет доступ к ресурсам знаний по различным аспектам ИКТР и обеспечивает интерактивное пространство для обмена знаниями и опытом, а также сотрудничество в продвижении ИКТР.

МОДУЛЬ 6

В информационный век информация является активом, который должен быть защищен, и людям, определяющим политику, надо знать, что означает информационная безопасность и какие действия предпринимать против утечки и нарушения законов об информации. Данный модуль дает общее представление о необходимости информационной безопасности, ее проблемах и направлениях и процессе формулирования стратегии по информационной безопасности.

Цели Модуля

Настоящий модуль преследует следующие цели:

1. Разъяснить концепцию информационной безопасности, конфиденциальности и связанные с ними понятия;

2. Рассмотреть угрозы информационной безопасности и возможные методы противодействия;

3. Обсудить требования для создания и внедрения политики информационной безопасности, а также жизненный цикл политики информационной безопасности;

4. Предоставить обзор существующих стандартов по информационной безопасности и защиты персональных данных, применяемых некоторыми странами и международными организациями по информационной безопасности.

Итоги обучения

После завершения изучения модуля читатели должны уметь:

1. Дать определение информационной безопасности, конфиденциальности и связанным с ними понятиям;

2. Идентифицировать угрозы информационной безопасности;

3. Давать оценку существующей политике информационной безопасности в свете международных стандартов по информационной безопасности и защиты персональных данных;

4. Формулировать или вносить рекомендации в отношении политики информационной безопасности, соответствующие по своему контексту.

СОДЕРЖАНИЕ

Список тематических исследований

Список рисунков

Список таблиц

Сокращения

APCERT	Азиатско-Тихоокеанская Служба реагирования на непредвиденные ситуации в компьютерах
АТУЦ ИКТР	Азиатско-Тихоокеанский учебный центр по информационным и коммуникационным технологиям для развития
APEC	Азиатско-Тихоокеанское экономическое сотрудничество
BPM	Руководство по базовому уровню защиты
BSI	Британский институт стандартов
BSI	Федеральное агентство по информационной безопасности, Германия
CAP	Авторизированный участник по сертификации
ОК	Общие критерии
CCP	Участники-потребители сертификатов
CCRA	Соглашение о признании сертификатов Общих критериев
КСЕК	Конвенция Совета Европы о киберпреступности
CERT	Служба реагирования на компьютерные инциденты
CERT/CC	Координационный центр службы реагирования на компьютерные инциденты
CIIP	Защита критической информационной инфраструктуры
CISA	Сертифицированный аудитор информационных систем
CISO	Главный управляющий по информационной безопасности
CISSP	Сертифицированный профессионал в области систем информационной безопасности
CM	Управление конфигурацией
CSEA	Акт о дополнительных мерах по обеспечению кибербезопасности
CSIRT	Служба реагирования на инциденты компьютерной безопасности
ГО	Глубокая оборона
DNS	Служба доменных имен
DoS	Отказ в обслуживании
ECPA	Акт о частной электронной связи
EGC	Европейская правительственная CERT
ENISA	Европейского агентства по сетевой и информационной безопасности
УРП	Управление рисками предприятия
ЭСКАТО	Экономическая и социальная комиссия ООН для Азии и Тихого океана
УБП	Управление безопасностью предприятия
ЕС	Европейский союз
FEMA	Федеральное агентство по чрезвычайным ситуациям, США
FIRST	Форум служб безопасности и реагирования на инциденты
FISMA	Акт о федеральном управлении информационной безопасностью
FOI	Свобода распространения информации
ГПК	Глобальная программа по кибербезопасности
HTTP	Протокол передачи гипертекстовых файлов
ИКТ	Информационные и коммуникационные технологии
ИКТР	Информационные и коммуникационные технологии для развития
IDS	Система по обнаружению вторжений
ФУИ	Форум по вопросам управления Интернетом
IM	Мгновенная передача сообщений
СПВ	Система предотвращения вторжения
ISACA	Ассоциация аудита и контроля информационных систем
СУИБ	Система управления информационной безопасностью
ISO/IEC	Международная организация по стандартизации/Международная электротехническая комиссия
ISP	Поставщик Интернет услуг

ISP/NSP	Поставщик услуг Интернет и сети
ИТ	Информационные технологии
МСЭ	Международный союз электросвязи
МСЭ-Д	Сектор развития международного союза электросвязи
МСЭ-Р	Сектор радиосвязи международного союза электросвязи
МСЭ-Т	Сектор стандартизации международного союза электросвязи
JTC	Группа технического комитета
KISA	Корейское агентство информационной безопасности
МИС	Министерство информации и связи, Республика Корея
СИБ	Сетевая и информационная безопасность
НЦИБ	Национальный центр по информационной безопасности, Япония
НИСТ	Национальный институт стандартов и технологий США
ОЭСР	Организация экономического сотрудничества и развития
АБУ	Административно-бюджетное управление, США
ОРП	Одноразовые пароли
ПК	Персональный компьютер
ПЗ	Профиль защиты
PSG	Постоянная группа заинтересованных сторон
RFID	Радиочастотная идентификация
КОБ	Компоненты обеспечения безопасности
ФТБ	Функциональные требования безопасности
МСП	Малые и средние предприятия
ЗБ	Задание по безопасности
TEL	Рабочая группа по телекоммуникациям и информации
ОО	Объект оценки
ФБОО	Функции безопасности ОО
UK	Соединенное Королевство
ООН	Организация Объединенных Наций
США	Соединенные штаты Америки
WPISP	Рабочая группа по информационной безопасности и неприкосновенности частной жизни
ВВУИО	Всемирная встреча на высшем уровне по вопросам информационного общества

Список условных обозначений

Тематическое исследование


Вопросы для размышления


Практическое упражнение

Проверьте себя

1. НЕОБХОДИМОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задачи данного раздела:
- **Объяснить понятия информации и информационной безопасности;**
- **Описать стандарты, применимые к деятельности по информационной безопасности.**

Человеческая жизнь сегодня сильно зависит от информационных и коммуникационных технологий (ИКТ). Это делает людей, организации и страны очень уязвимыми при атаках на информационные системы, таких как: хакерство (взлом), кибертерроризм, киберпреступления и т.п. Немного людей и организаций имеют соответствующие средства для борьбы с такими нападениями. Правительства призваны сыграть важную роль в обеспечении информационной безопасности, расширяя информационно-коммуникационную инфраструктуру и устанавливая системы защиты от угроз информационной безопасности.

1.1 Основные понятия в информационной безопасности

Что такое «информация»?

Как правило, информация определяется как результат умственной деятельности; это нематериальный продукт, который передается через средства массовой информации (СМИ). В области ИКТ информация является результатом обработки, манипулирования и организации данных, которые являются просто набором фактов.

В области информационной безопасности информация определяется как «актив», который имеет добавочную стоимость и вследствие этого нуждается в защите . В данном модуле используется определение информации и информационной безопасности, приведенное в международном стандарте ISO/IEC 27001.

Значение, придаваемое информации сегодня, свидетельствует о переходе от сельскохозяйственного общества к индустриальному и, в конечном итоге, к информационно-ориентированному обществу. При сельскохозяйственном обществе земля была самым важным активом, и страна с высоким уровнем производства зерна имела конкурентное преимущество. В индустриальном обществе ключевым фактором конкурентоспособности является сила капитала, например, запасы нефти. В обществе, ориентируемом на знания и информацию, последняя является важнейшим активом, а возможность собирать, анализировать и использовать информацию дает конкурентное преимущество любой стране.

Так как перспективы были смещены от стоимости чистых активов к стоимости информационных активов, растет понимание того, что информация должна быть защищена. Информация сама по себе оценивается выше, чем та, которая содержится в СМИ. В таблице 1 приводятся различия между информационными и материальными ресурсами.

Таблица 1. Сравнение информационных и материальных активов

Характерные признаки	Информационные активы	Материальные активы
Сохранение формы	Не имеют физической формы и могут меняться	Имеют физическую форму
Непостоянство ценности	Получение высокой стоимости при объединении и обработке	Общая стоимость представляет собой сумму стоимостей всех ресурсов
Совместное использование	Возможно неограниченное размножение информационных активов, и люди могут совместно их использовать	Воспроизводство является невозможным; стоимость активов при размножении снижается
Зависимость от средств связи	Должна быть доставлена с помощью средств связи	Может быть доставлена самостоятельно (в соответствии с физической формой)

Как показано в таблице 1, информационные ресурсы радикально отличаются от материальных активов. Таким образом, информационные активы уязвимы для различного рода рисков.

Риски по отношению к информационным ресурсам

Поскольку ценность информационных активов повышается, желание людей получить доступ к информации и контролировать ее нарастает. Формируются группы для использования информационных активов в различных целях, и некоторые прилагают усилия, чтобы завладеть ими любыми способами. К последним относятся взлом, компьютерное пиратство, разрушение информационных систем посредством компьютерных вирусов и другие. Данные риски, которые сопровождают процесс информатизации, рассматриваются в разделе 2 настоящего модуля.

Негативные аспекты информационно-ориентированной среды включают в себя следующее:

Увеличение неэтичного поведения в связи с анонимностью - ИКТ может использоваться для сохранения анонимности, что облегчает для определенных людей неэтичное и преступное поведение, в том числе незаконное приобретение информации.

Конфликты по вопросам собственности и управления информацией - Осложнения, вызванные вопросами собственности и контроля информации, увеличились с распространением информатизации. Например, поскольку правительства стремятся построить базу данных персональной информации в рамках построения «электронного правительства», многие выразили обеспокоенность по поводу возможности вторжения в частную жизнь при разглашении личной информации другим лицам.

Разница между классами и странами по доступу к информационным и финансовым ресурсам - Размер наличия информационных активов может быть показателем богатства в обществах, ориентируемых на знания/информацию. Развитые страны

имеют потенциал для получения дополнительной информации и прибыли от продажи информации в качестве продукта. С другой стороны, информационно-бедные страны нуждаются в крупных инвестициях только для того, чтобы быть в состоянии получить доступ к информации.

Растущая незащищенность информации, вызванная современными сетями - Общество, которое ориентируется в своем развитии на знания/информацию, представляет собой сетевое общество. Весь мир связан в единую сеть, а это означает, что слабости в одной ее части могут неблагоприятно отразиться на остальной части сети.

Что такое информационная безопасность?

В ответ на попытки получить информацию незаконно, люди прилагают усилия для предотвращения информационно-связанных преступлений или минимизации ущерба, который могут нанести такие преступления. Это называется информационной безопасностью.

Проще говоря, информационная безопасность признает ценность информации и защищает ее.

4П информационной безопасности

Четыре П информационной безопасности - это Правильная информация, Правильные люди, Правильное время и Правильная форма. Контроль над четырьмя П является наиболее эффективным способом поддержания и управления ценностью информации.

Рисунок 1. 4П информационной безопасности

«Правильная информация» относится к точности и полноте информации, которая гарантирует достоверность (целостность) информации.

«Правильные люди» подразумевает, что информация доступна только уполномоченным людям, что гарантирует конфиденциальность.

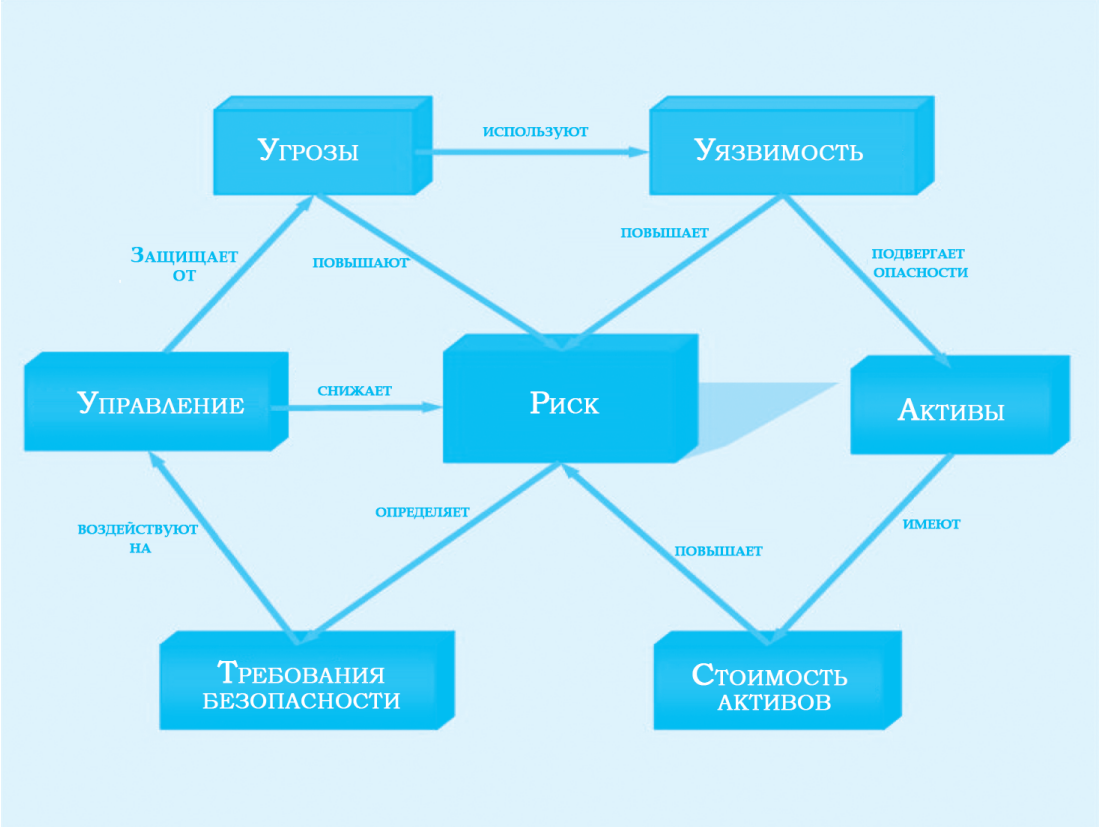
«Правильное время» указывает на доступность информации, удобство и простоту ее использования по требованию уполномоченного органа. Это гарантирует доступность.

«Правильная форма» относится к предоставлению информации в нужном формате.

Для обеспечения информационной безопасности четыре П должны применяться правильно. Это означает, что при работе с информацией должны соблюдаться конфиденциальность, целостность и доступность.

Информационная безопасность также требует ясного понимания ценности информационных активов, а также их уязвимости и соответствующих угроз. Это известно как управление рисками. Рисунок 2 показывает взаимосвязь между информационными ресурсами и рисками.

Рисунок 2. Взаимосвязь между рисками и информационными ресурсами



Риск определяется на основе стоимости активов, угроз и уязвимостей. Применяется следующая формула:

Риск = $\int$ (Стоимость активов, Угрозы, Уязвимости)

Риск прямо пропорционален стоимости активов, угрозам и уязвимости. Таким образом, риск может быть увеличен или уменьшен путем манипулирования размером стоимости активов, угроз и уязвимости. Это может быть сделано на основе управления рисками.

Существуют следующие методы управления рисками:

Снижение риска (смягчение риска) - это выполняется, когда вероятность угроз/уязвимости высокая, но их воздействие является низким. Это предполагает понимание угрозы и уязвимости, их изменение или уменьшение и осуществление мер противодействия. Тем не менее, снижение риска не уменьшает значение риска до нуля.

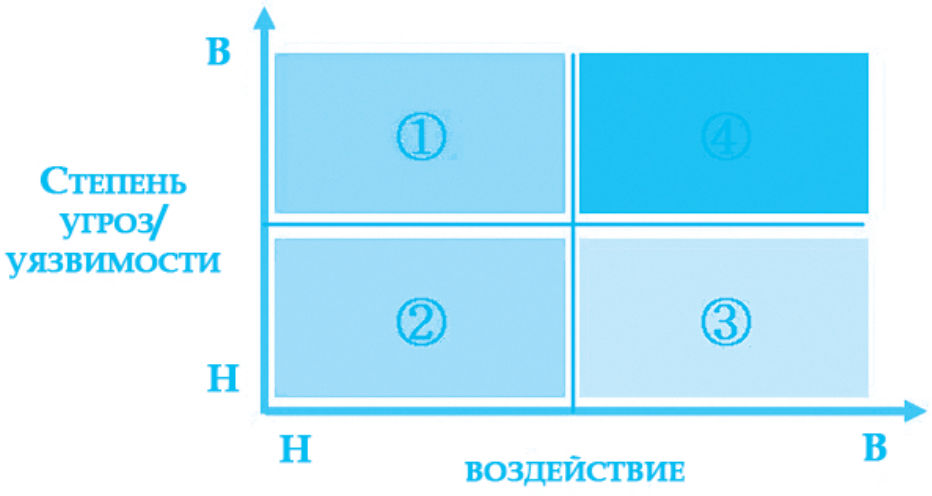
Принятие риска - это выполняется, когда вероятность угроз/уязвимости низкая, и их вероятное воздействие является незначительным или допустимым.

Перенос риска - если риск слишком высокий или организация не в состоянии подготовить необходимые средства контроля, риск может быть перенесен за пределы организации. Одним из примеров является получение страхового полиса.

Избежание риска - если угрозы и уязвимости весьма вероятны и их влияние также чрезвычайно высоко, лучше избегать риска путем аутсорсинга, например, оборудования обработки данных и персонала.

Графическое представление этих четырех методов управления рисками показано на рисунке 3. На данном рисунке квадрант с пометкой «1» означает снижение риска, «2» - принятие риска, «3» - перенос риска и «4» - избежание риска.

Рисунок 3. Методы управления рисками



Ключевым рассмотрением при выборе соответствующего метода управления рисками является рентабельность. Анализ рентабельности должен быть выполнен перед принятием плана по снижению, принятию, переносу или избеганию риска.

1.2 Стандарты деятельности по обеспечению информационной безопасности

Деятельность по обеспечению информационной безопасности не может быть эффективно выполнена без мобилизации единого административного, физического и технического плана.

Многие организации рекомендовали стандарты деятельности для обеспечения информационной безопасности. Наглядными примерами являются требования информационной безопасности Международной организации по стандартизации и Международной электротехнической комиссии , критерии оценки сертифицированного Аудитора Информационных систем и сертифицированного Профессионала в области систем информационной безопасности от Ассоциации аудита и контроля информационных систем. Эти стандарты рекомендуют такие унифицированные деятельности для информационной безопасности, как разработка политики в области информационной безопасности, создание и функционирование организации по информационной безопасности, управление человеческими ресурсами, физической безопасностью и технической безопасностью, управление аудитом безопасности и непрерывностью бизнес-деятельности.

В таблице 2 перечислены стандарты, связанные с областью информационной безопасности.

Таблица 2. Домены информационной безопасности и связанные с ними стандарты

Домены безопасности	ISO/IEC 27001	CISA	CISSP
Административные	• Политика безопасности	• ИТ-управление	• Методы управления безопасностью • Архитектура и модели безопасности
	• Организация информационной безопасности	• ИТ-управление	
	• Управление активами	• Защита информационных ресурсов	• Методы управления безопасностью
	• Безопасность человеческих ресурсов		
	• Управление инцидентами информационной безопасности	• Бизнес-непрерывность и восстановление	• Планирование бизнес-непрерывности и восстановления после аварий
	• Управление бизнес-непрерывностью	• Бизнес-непрерывность и восстановление после аварий	• Планирование бизнес-непрерывности и восстановления после аварий
	• Соответствие	• Процесс контроля информационной безопасности	• Право, расследование и этика
Физические	• Физическая безопасность и безопасность окружающей среды		• Физическая безопасность
Технические	• Управление коммуникациями и операциями	• Управление жизненным циклом систем и инфраструктур	• Криптография • Телеммуникационная и сетевая безопасность • Безопасность операций
	• Контроль доступа		
	• Приобретение, разработка и эксплуатация информационных систем	• Поставка и поддержка услуг в области ИТ	

Стандарт ISO/IEC27001[1] в основном рассматривает вопросы административной безопасности. В частности, особое внимание уделяется вопросам аудита документирования и деятельности в качестве административного поведения и соблюдения политики/директивы и закона. Требуется непрерывное подтверждение и меры противодействия со стороны администратора. Таким образом, ISO/IEC27001 пытается устранить слабые места в системах обеспечения безопасности, оборудовании и т.п. в административном порядке. .

Напротив, нет никакого упоминания о человеческих ресурсах или физической безопасности в CISA,[2] в котором основное внимание уделяется аудиторской деятельности и контролю над информационными системами. Соответственно, роль аудиторов и эффективность процесса проверки являются весьма важными.

CISSP[3] уделяет внимание, в основном, технической безопасности. Он подчеркивает значение организации и контроля работы оборудования, как серверы или компьютеры.

Практическое упражнение

1. Оцените уровень понимания информационной безопасности среди персонала вашей организации.

2. Какие меры по информационной безопасности осуществляет ваша организация? Классифицируйте эти меры с точки зрения четырех методов информационной безопасности.

3. Приведите примеры мер по обеспечению информационной безопасности в административных, физических и технических областях в рамках вашей организации или в других организациях вашей страны или юрисдикции.

Участники могут выполнить эти упражнения в небольших группах. Группы могут быть сформированы в зависимости от стран, из которых прибыли участники.

Проверьте себя

1. Как информация отличается от других ресурсов?

2. Почему информационная безопасность относится к вопросам политики?

3. Каковы способы обеспечения информационной безопасности? Определите различные методы решения проблемы информационной безопасности.

4. Проведите различия между каждой из трех областей информационной безопасности (административной, физической и технической).

1 ISO, “ISO/IEC27001:2005,” http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.
2 See ISACA, “Standards for Information Systems Auditing,” http://www.isaca.org/Template.cfm?Section=CISA_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=19566.
3 See (ISC)², “CISSP® - Certified Information Systems Security Professional,” http://www.isc2.org/cissp.

2. ТЕНДЕНЦИИ И НАПРАВЛЕНИЯ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задачи данного раздела:
- **Дать обзор угроз информационной безопасности;**
- **Описать меры противодействия таким угрозам.**

2.1 Виды нападений на системы обеспечения информационной безопасности

Хакинг

Хакинг (проникновение в компьютерную систему) – это действие с целью получения доступа к компьютеру или компьютерной сети для получения или изменения информации без законного разрешения.

В зависимости от цели нападения хакинг может быть классифицирован как развлекательный, преступный или политический взлом. Развлекательный взлом – это несанкционированное изменение программ и данных, чтобы просто удовлетворить хакерское любопытство. Преступный взлом используется в мошенничестве или шпионаже. Политический взлом связан с вмешательством в функционирование вебсайтов с целью транслирования несанкционированных политических сообщений.[4]

В последнее время взлом стал все больше ассоциироваться с кибертеррором и кибервойной, что создает серьезную угрозу национальной безопасности.

4 Suresh Ramasubramanian, Salman Ansari and Fuatai Purcell, “Governing Internet Use: Spam, Cybercrime and e-Commerce,” in Danny Butt (ed.), *Internet Governance: Asia-Pacific Perspectives* (Bangkok: UNDP-APDIP, 2005), 95, http://www.apdip.net/projects/igov/ICT4DSeries-iGov-Ch5.pdf.

Американо-китайская сетевая война

Американская хакерская группа PoizonBox обвинялась в повреждении более чем 350 китайских вебсайтов в течение месяца. 30 апреля 2001 года в течение дня эта группа также якобы напала на 24 китайских вебсайта, включая сайты восьми китайских правительственных организаций. Тогда китайские хакеры объявили Шестую Сетевую войну Национальной обороны и в течение недели с 30 апреля до 1 мая 2001 года атаковали американские вебсайты, включая сайты американских правительственных организаций. Нападения были таковы, что Пентагон поднял статус безопасности своих компьютерных систем от нормальной INFO-CON NORMAL до повышенной опасности INFO-CONALPHA. ПО состоянию на 1 мая 2001 года Национальный центр защиты инфраструктуры Федерального бюро расследований США выпустил предупреждение о том, что китайские хакеры поражают сайты американского правительства и компаний.

После сетевой войны США признали, что электронные угрозы (например, взлом) могут причинить большой ущерб американским правительственным организациям, и впоследствии усилили защиту от киберугроз, увеличивая бюджет информационной безопасности и совершенствуя информационную политику внутри правительственных организаций.

Источник:Attrition.org, «Кибервойна с Китаем: сбывающееся пророчество» (2001 г.), http://attrition.org/security/commentary/cn-us-war.html.

Отказ в обслуживании

Атаки отказа в обслуживании (DoS - Denial-of-service) препятствуют использованию услуг законным пользователям, в то время как преступник получает несанкционированный доступ к машинам или данным. Это происходит, когда атакующие «наводняют» сеть большими объемами данных или преднамеренно потребляют недостаточные или ограниченные ресурсы, такие как: блоки управления процессами или ожидаемое соединение сети. Либо они могут нарушить физические компоненты сети или манипулировать данными при передаче, в том числе зашифрованные данные.[5]

5 ESCAP, “Module 3: Cyber Crime and Security,” http://www.unescap.org/icstd/POLICY/publications/internet-use-for-business-development/module3-sources.asp.

Кибертеррор против Эстонии

4 мая 2007 года в столице Эстонии перенос памятника Победы СССР из центра города на военное кладбище вызвал трехнедельную атаку кибертеррора против Эстонии, состоящую из DoS-атак на миллион компьютеров. Компьютерная сеть и сайты президентской резиденции, парламента Эстонии, различных государственных ведомств, правящей партии, прессы и банков подверглись нападению. Даже беспроводная сеть подверглась атаке.

Эстония позже выяснила, что месторасположением злоумышленников была российская государственная организация. Но Российское правительство отвергло обвинения.

Когда развернулось нападение кибертеррористов, Эстония оказалась неспособной оперативно среагировать из-за отсутствия соответствующей аварийной службы и политики в области информационной безопасности.

Источник: Beatrix Toth, «Эстония под воздействием кибер-атак» (Hun-CERT, 2007г.), http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

Вредоносный код

Вредоносный код относится к программам, выполнение которых приводит к повреждению системы. Вирусы, «черви» и «Троянские кони» являются типами вредоносного кода.

Компьютерный **вирус** представляет собой компьютерную программу или программный код, который повреждает компьютерные системы и данные путем копирования самого себя в другую программу, компьютерный загрузочный сектор или документ.

«Червь» представляет собой самовоспроизводящийся вирус, который не изменяет файлы, но находится в активной памяти, используя части операционной системы, которые являются автоматическими и обычно невидимы для пользователя. Их бесконтрольное распространение потребляет ресурсы системы, замедляя или останавливая другие задачи. Это, как правило, происходит только тогда, когда присутствие червей обнаружено.

«Троянский конь» является программой, которая может быть полезна и/или безвредна, но в действительности имеет вредоносные функции, такие как: загрузка скрытых программ или последовательности команд, что делает систему уязвимой для вторжения.

Интернет-кризис 1.25 в Республике Корея

25 января 2003 года компьютерный вирус под названием «червь Slammer» стал причиной прекращения подключений к Интернету по всей Республике Корея. Остановка, которая продолжалась более девяти часов, была вызвана повреждением службы сервера доменных имен (DNS), нанесенным «червем».

В результате прекращения подключения онлайн-магазины потеряли приблизительно 200-500 тыс. долларов США, и потери в онлайн-торговле составили 22,5 млрд. долларов США. Сообщалось, что ущерб, нанесенный червем Slammer, был больше ущерба, причиненного червями Codred и Nimda, где жертвами были обычные пользователи.

Интернет-кризис заставил корейское правительство разработать всестороннюю систему по управлению поставщиками услуг интернета (ISP) и службой информационной безопасности. Были установлены системы защиты информационной инфраструктуры и оценки информационной безопасности и учреждены подразделения или комитеты по информационной безопасности в каждой организации.

Социальная инженерия

Термин «социальная инженерия» относится к ряду методов, используемых для манипулирования людьми для получения конфиденциальной информации. Хотя это похоже на мошенничество или просто обман, данный термин обычно применяется в случае мошенничества с целью сбора информации или доступа к компьютерной системе. В большинстве случаев злоумышленник никогда не встречается лицом к лицу с жертвой.

Фишинг, действие кражи персональной информации через Интернет с целью совершения финансового мошенничества, является примером социальной инженерии. Фишинг стал существенной преступной деятельностью в Интернете.

Шведский банк подвергся «крупнейшему» онлайн-грабежу

19 января 2007 года шведский банк Nordea подвергся онлайн-фишингу. Атака была инициирована специально написанным «Троянцем», отправленным от имени банка некоторым из его клиентов. Отправитель предлагал клиентам скачать программу по «борьбе со спамом». Пользователи, которые загрузили приложенный файл под названием «raking.zip» или «raking.exe», заразили свои компьютеры «Троянцем», также известным некоторым службам безопасности как «haxdoor.ki».

Haxdoor обычно устанавливает логгер клавиатуры , чтобы сделать запись нажатий клавиши и скрывает себя с помощью руткитов . Троян с расширением .ki активизировался в том случае, если пользователи пытались открыть сайт банка Nordea. Пользователи перенаправлялись на ложную вебстраницу, где они вводили важную информацию логина, включая номера логина. После того, как пользователи вводили информацию, появлялось сообщение об ошибке, в котором говорилось, что сайт испытывает технические проблемы. Затем преступники использовали собранные данные клиентов на настоящем вебсайте Nordea, чтобы снять деньги с их счетов.

Клиенты Nordea были подвержены вреду по электронной почте, содержащей сделанный на заказ вирус, в течение 15 месяцев. Общие убытки двухсот пятидесяти клиентов банка, которых, как утверждалось, коснулось это, составили от семи до восьми миллионов шведских крон (7300-8300 долларов США). Этот случай доказывает, что кибератаки могут затронуть даже финансовые компании с высоким уровнем защиты.

Источник: Tom Espiner, «Шведский банк подвергся «крупнейшему» онлайн-грабежу», *ZDNet.co.uk* (19 January 2007), http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm

2.2 Тенденции угроз в области информационной безопасности[6]

Важным направлением деятельности в обеспечении информационной безопасности является анализ тенденций угрозы безопасности. Это относится к рассмотрению моделей угроз безопасности в течение долгого времени, чтобы определить пути, по которым такие модели изменяются и развиваются, меняют движение в новых направлениях, или смещаются. Данный повторяющийся процесс сбора и сопоставления информации и улучшения осведомленности об инциденте осуществляется для прогнозирования вероятных или возможных угроз и подготовки соответствующего ответа на эти угрозы.

К организациям, которые занимаются анализом тенденций угроз информационной безопасности и совместно используют отчеты о тенденции угрозы безопасности, относятся:

- CERT (http://www.cert.org/cert/)
- Symantec (http://www.symantec.com/business/theme.jsp?themeid=threatreport)
- IBM (http://xforce.iss.net/)

6 This section is drawn from Tim Shimeall and Phil Williams, *Models of Information Security Trend Analysis* (Pittsburgh: CERT Analysis Center, 2002), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.

Тенденции в области угроз информационной безопасности, которые были зарегистрированы, описаны ниже.

Автоматизация средств нападения[7]

Злоумышленники в настоящее время используются автоматизированные средства, которые позволяют им быстро и легко собирать информацию о тысячах Интернет-серверов. Сети могут быть отсканированы с удаленного местоположения, и хосты с определенными слабостями идентифицируются с использованием этих автоматизированных инструментов. Злоумышленники заносят в каталог информацию для дальнейшего использования, передают или продают ее другим, или незамедлительно нападают. Некоторые инструменты (такие, как cain&abel) автоматизируют ряд небольших нападений на общую цель. Например, злоумышленники могут использовать анализатор пакетов (packet sniffer) для получения паролей к маршрутизаторам или брандмауэру, доступа к брандмауэру, чтобы отключить фильтры, а затем использовать сетевую файловую службу для чтения данных на сервере.

Средства нападения, которые трудно обнаружить

Некоторые средства атаки используют новые схемы нападения, которые не определяются существующими инструментами обнаружения. Например, методы, не подлежащие судебному преследованию, используются, чтобы замаскировать или скрыть природу средств нападения. Полиморфные средства изменяют форму каждый раз, когда они используются. Некоторые из них используют общие протоколы, как протокол передачи гипертекста (HTTP), что мешает отличить их от легального сетевого трафика.[8] Хорошим примером является червь в программе MSN Messenger. Червь из клиентской программы мгновенного обмена сообщениями MSN Messenger посылает по контактным данным из адресной книги зараженного пользователя файл, предназначенный для заражения систем, после первого же предупреждения о том, что они вот-вот получат файл. Имитируется поведение реального пользователя программы мгновенного обмена сообщениями, что вызывает тревогу.[9]

Более быстрое обнаружение уязвимостей

Ежегодно число вновь обнаруженных уязвимостей в программных продуктах, о которых доводится до сведения Координационного центра службы реагирования на компьютерные инциденты (CERT/CC), более чем удваивается в количестве, что создает трудности администраторам не отставать со своими «заплатками». Злоумышленники знают это и пользуются преимуществом.[10] Некоторые нарушители начинают атаку в выбранный день (или выбранный час), которая представляет собой угрозу, использующую уязвимость компьютерных приложений, для которых нет «заплат» или защиты, поскольку они еще не были обнаружены администраторами.[11]

Увеличение асимметричной угрозы и конвергенция методов нападения

Асимметричной угрозой является состояние, при котором злоумышленник имеет преимущество перед защитником. Число ассиметричных угроз возрастает с автоматизацией применения угрозы и совершенствованием средств нападения.

7 This section is drawn from CERT, “Security of the Internet,” Carnegie Mellon University, http://www.cert.org/encyc_article/tocencyc.html
8 Suresh Ramasubrahmanian et al., op. cit., 94.
9 Munir Kotadia, “Email worm graduates to IM,” *ZDNet.co.uk* (4 April 2005), http://news.zdnet.co.uk/security/0,1000000189,39193674,00.htm.
10 Suresh Ramasubrahmanian et al., op. cit.
11 Wikipedia, “Zero day attack,” Wikimedia Foundation Inc., http://en.wikipedia.org/wiki/Zero_day_attack.

Конвергенция методов нападения указывает на объединение разнообразных методов нападения с целью создания глобальной сети, которая поддерживает скоординированную вредоносную деятельность. Одним из примеров является Mpack, «троянец», который устанавливается на компьютере пользователя посредством установления контакта с серверами MPack. Злоумышленник генерирует трафик к этим серверам в ущерб законным сайтам таким образом, чтобы посетители этих сайтов были перенаправлены к вредоносным веб-серверам, или отправляет ссылки на вредоносные веб-серверы на основе спам-сообщений. Эти вредоносные серверы перенаправляют браузер пользователей к серверам MPack.[12]

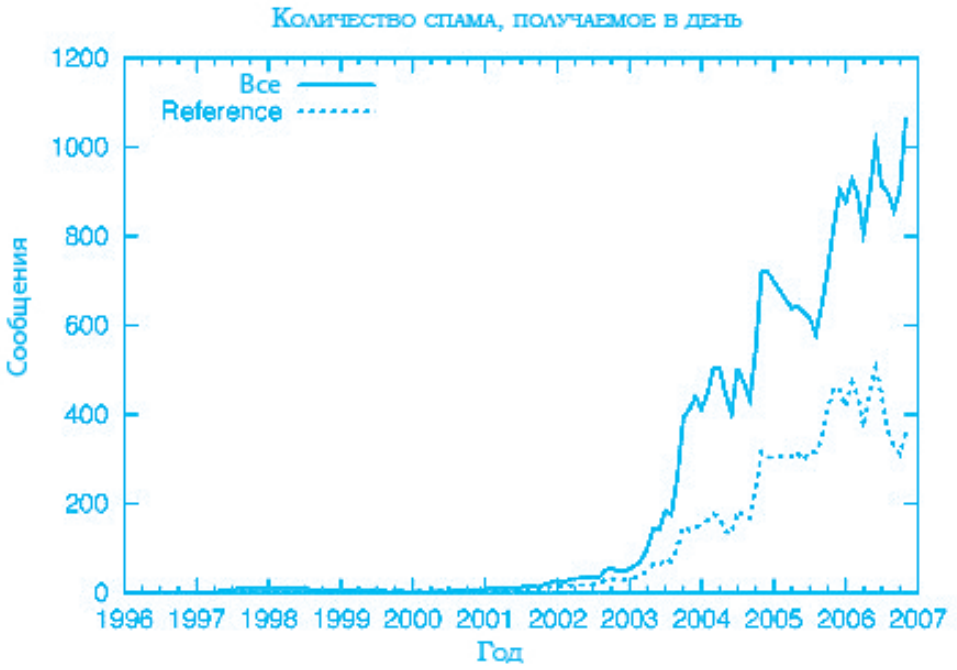
Увеличение угрозы нападения на инфраструктуры

Нападения на инфраструктуры – это атаки, которые широко затрагивают ключевые компоненты Интернета. Они вызывают озабоченность из-за количества организаций и пользователей в Интернете и их увеличивающейся зависимости от Интернета для выполнения повседневных дел. Результатом нападения на инфраструктуру могут быть DoS-атаки, дискредитация конфиденциальной информации, распространение дезинформации, а также значительное отвлечение ресурсов от выполнения других задач.

Ботнет (Botnet) является примером нападения на инфраструктуру. Термин «botnet» относится к группе зараженных компьютеров, управляемых удаленно «сервером управления командами». Зараженные компьютеры распространяют «черви» и «трояны» через сетевые системы.

Спам быстро растет в связи с использованием ботнет. Спам относится к незапрашиваемой массе сообщений, которые могут быть отправлены через электронную почту, мгновенные сообщения, поисковые системы, блоги и даже мобильные телефоны. Рисунок 4 показывает тенденцию изменения объемов спама.

Рисунок 4. Статистика спама



12 Symantec, *Symantec Internet Security Threat Report: Trends for January–June 07*, Volume XII (September 2007), 13, http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf.

Противодействие ботнет

Чтобы уменьшить ущерб от действия ботнет, Международный союз электросвязи (МСЭ) рекомендует использовать сочетание политики, технологии и социальной методологии.

Политические методы: эффективные законы и нормативы антиспаму и киберпреступлениям

- Создание потенциала среди соответствующих политических заинтересованных сторон
- Всеобъемлющая база для международного сотрудничества и информационно-пропагандистской деятельности
- Соответствие между законодательством о киберпреступности и неприкосновенности частной жизни
- Комплекс мер местного осуществления наказания киберпреступлений и подавления сетей ботнет

Технические методы: средства и методы для обнаружения и сбора информации об активных сетях ботнет

- Передовой опыт поставщиков услуг Интернета по уменьшению воздействия сетей ботнет
- Передовой опыт регистраров и регистраторов по уменьшению воздействия сетей ботнет
- Наращивание потенциала для электронной коммерции и провайдеров онлайн-транзакций

Социальные методы: широкомасштабные образовательные инициативы в области Интернет-безопасности и защиты

- Содействие обеспечению безопасного доступа к ИКТ для пользователей

Инструментарий PTF ITU SPAM представляет собой комплексный пакет для оказания помощи разработчикам политики, управляющим и компаниям в регулировании политики и восстановлении доверия к электронной почте. Данный набор инструментариев также рекомендует обмен информацией между странами в целях предотвращения международных проблем.

Изменение целей атак

Раньше считалось, что компьютерные и сетевые атаки совершались из любопытства или самодовольства. Теперь целями являются, как правило, деньги, клевета и разрушение. Кроме того, эти виды атак представляют собой лишь небольшую часть широкого спектра киберпреступности.

Киберпреступностью является преднамеренное уничтожение, разрушение или искажение цифровых данных или информационных потоков по политическим, экономическим, религиозным или идеологическим причинам. Наиболее распространенные преступления включают взлом, DoS-атаки, вредоносный код и социальную инженерию. Недавно киберпреступность стала частью кибертеррора и кибервойн, что негативно сказывается на национальной безопасности.

Таблица 3 показывает, какой доход получают киберпреступники.

Таблица 3. Доходы от киберпреступлений в 2007 г.

Активы	Уровень цен (в долл. США)
Выплаты за установку каждого бесплатного программного продукта	30 центов в США, 20 центов в Канаде, 10 центов в Великобритании, 2 цента в других странах
Пакет вредоносных программ, базовая версия	1000–2000 долл. США
Пакет вредоносных программ с дополнительными услугами	Варьирование цен от 20 долл. США и выше
Аренда за использование оборудования – 1 час	0,99 – 1 долл. США
Аренда за использование оборудования – 2,5 часа	1,60 – 2 долл. США
Аренда за использование оборудования – 5 часов	4 долл. США, цена может варьироваться
Необнаруженная копия конкретного Трояна для кражи информации	80 долл. США, цена может варьироваться
Распространенные DoS-атаки	100 долл. США за день
10,000 зараженных ПК	1000 долл. США
Данные украденного банковского счета	Варьирование цен от 50 долл. США
1 миллион свежесобранных e-mail адресов (не проверено)	свыше 8 долл. США, в зависимости от качества

Источник:Trend Micro, *2007 Threat Report and Forecast* (2007), 41, http://trendmicro.mediaroom.com/file.php/66/2007+Trend+Micro+Report_FINAL.pdf

2.3 Повышение безопасности

Учитывая тенденции в области угроз безопасности и технологий нападений, прочная защита требует гибкой стратегии, которая дает возможность адаптации к изменяющимся условиям, четкой политики и процедур, использование соответствующих технологий безопасности и постоянную бдительность.

Целесообразно начинать программу усовершенствования безопасности путем определения текущего состояния безопасности. Целостность программы безопасности – это документально оформленные политики и процедуры, а также технологии, которые поддерживают их внедрение.

Административная безопасность

Административная безопасность состоит из стратегии информационной безопасности, политики и руководящих принципов.

Стратегия по информационной безопасности определяет направление для всех мероприятий по информационной безопасности.

Политика в области информационной безопасности представляет собой документированный план высокого уровня по информационной безопасности в рамках организации. Это служит основой для принятия конкретных решений, таких как план административной и физической безопасности.

Поскольку политика информационной безопасности должна быть долгосрочной, она должна избегать технологически определенного содержания и включать в себя эффективное развитие планирования по обеспечению непрерывности бизнеса.

Руководящие принципы по информационной безопасности должны быть установлены в соответствии со стратегией и политикой в области информационной безопасности. Руководящие принципы должны точно определять правила для каждой из областей, связанных с информационной безопасностью. И потому, что руководящие принципы должны быть всеобъемлющими и в национальном масштабе, они должны быть разработаны и донесены правительством для соблюдения их организациями.

Стандарты информационной безопасности должны быть специализированы и определены так, чтобы они могли быть применены ко всем областям информационной безопасности. Для каждой страны желательно разработать собственные стандарты после анализа стандартов административной, физической и технической безопасности, которые широко используются во всем мире. Стандарты должны соответствовать существующей среде в ИКТ.

Стратегия информационной безопасности страны, политика и руководящие принципы должны быть в соответствии с соответствующими законами. Их область действия должна находиться в пределах национальных и международных законов.

Функционирование и процессы по обеспечению информационной безопасности

Как только стратегия, политика и руководящие принципы по информационной безопасности будут созданы, должны быть определены рабочие процедуры и регламенты по обеспечению информационной безопасности. Поскольку люди являются теми, кто совершают атаки на информацию или ответственны за утечку внутренней информации, управление человеческими ресурсами является наиболее важным фактором в работе по обеспечению информационной безопасности. Следовательно, возникает необходимость в следующем:

1. Программа образования и обучения информационной безопасности – Есть много способов для улучшения уровня информационной безопасности организаций, но основными являются образование и обучение. Члены организации должны понимать необходимость в информационной безопасности и приобретать соответствующие навыки через образование и профессиональную подготовку. Тем не менее, важно развивать различные программы для достижения максимального учатия, так как стандартные программы образования и обучения информационной безопасности могут быть неэффективные.

2. Усиление поощрения с помощью различных мероприятий – Участие сотрудников имеет важное значение для успешной реализации стратегии, политики и руководящих принципов по информационной безопасности. Информационная безопасность должна пропагандироваться среди сотрудников с помощью различных повседневных мероприятий.

3. Обеспечение спонсорской поддержки – Несмотря на то, что может быть высокий уровень понимания информационной безопасности среди сотрудников и наличия у них сильного желания поддерживать информационную безопасность, трудно обеспечивать информационную безопасность без поддержки со стороны высшего руководства организации. Должна быть получена поддержка со стороны главного исполнительного директора и главного сотрудника по вопросам информации (CIO).

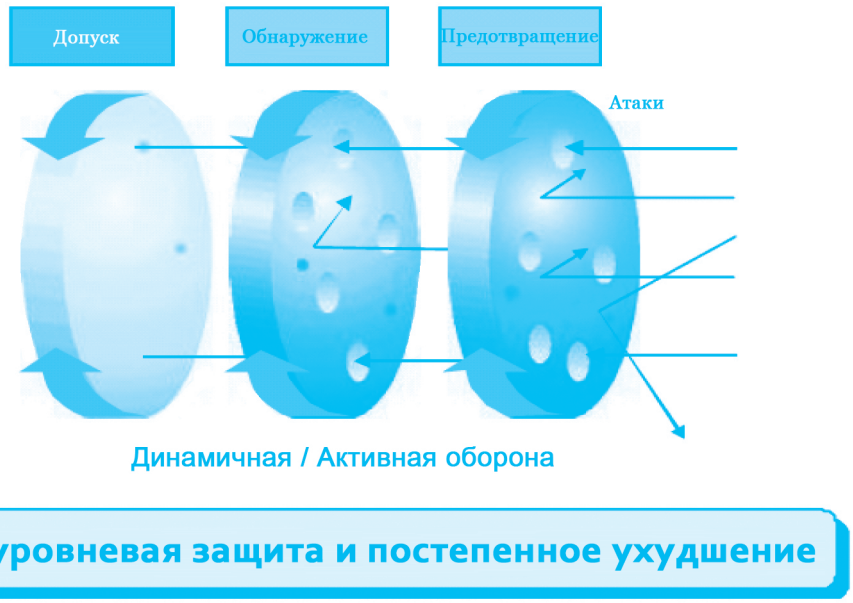
Технологическая безопасность

Для помощи организациям по защите своих информационных систем от злоумышленников были разработаны различные технологии. Данные технологии помогают защитить системы и информацию от нападений, выявлять необычную или подозрительную деятельность и реагировать на события, которые влияют на безопасность.

Сегодняшние системы обеспечения безопасности были спроектированы и разработаны на основе модели «Глубокая оборона» (ГО – Defense-In-Depth или DID), которая приводит к единому управлению связанных технологий. Данная модель отличается от защиты по периметру безопасности, которая имеет только один уровень защиты против всех угроз. Модель ГО состоит из предотвращения, обнаружения и допуска, где на каждом этапе угрозы снижаются (рис. 5).

Рисунок 5. Глубокая оборона

(Источник: Defense Science Board, *Protecting the Homeland: Defensive Information Operations 2000 Summer Study Volume II* (Washington, D.C.: Defense Science Board, 2001), 5, http://www.acq.osd.mil/dsb/reports/dio.pdf)



Технологии предотвращения

Технологии предотвращения защищают от вторжений и угроз на уровне хранения или системы. Эти технологии включают в себя следующее:

1. Криптография, также называемая шифрованием, – это процесс преобразования информации из первоначальной формы (называемой текстом) в закодированную, недоступную форму (называемую зашифрованным текстом). Декодирование относится к процессу принятия зашифрованного текста и перевода его в обычный текст. Криптография используется для защиты различных приложений. Более подробную информацию о криптографии и связанных технологиях (IPSec, SSH, SSL, VPN, OTP, и т.д.) можно найти на следующих веб-страницах:

    - IETF RFC (http://www.ietf.org/rfc.html)
    - Часто задаваемые вопросы лаборатории RSA о современной криптографии (http://www.rsa.com/rsalabs/node.asp?id=2152)

2. Одноразовые пароли (ОРП) – Как видно из названия, одноразовые пароли могут использоваться только один раз. Статические пароли могут быть более легко доступными из-за потери пароля, перехвата пароля, взлома пароля и т.п. Данный риск может быть значительно снижен, если постоянно менять пароль, как это делается с ОРП. По этой причине ОРП используется для безопасных электронных финансовых транзакций, таких как банковское обслуживание в онлайн-режиме (онлайн-банкинг).

3. Брандмауэры – Брандмауэры регулируют часть потока движения между компьютерными сетями различных уровней доверия: между Интернетом, который является зоной недоверия, и внутренней сетью, которая является зоной высшего доверия. Зону с промежуточным уровнем доверия, расположенной между Интернетом и внутренней доверенной сетью, часто называют «сетью по периметру» или демилитаризированной зоной.

4. Средства анализа уязвимости – Из-за увеличения количества методов нападения и уязвимостей, представленных в широко используемых приложениях, необходимо периодически проводить оценку уязвимости системы. В компьютерной безопасности уязвимость является слабостью, которая позволяет злоумышленнику получить доступ к нарушению системы. Уязвимости могут быть вызваны слабыми паролями, ошибками программного обеспечения, компьютерными вирусами, внедрениями скрипт-кода, внедрениями SQL-кода или вредоносных программ. Средства анализа обнаруживают такие уязвимости. Они легко доступны в онлайне, и существуют компании, которые оказывают аналитические услуги. Тем не менее, те, которые находятся в свободном доступе для интернет-сообщества, могут быть использованы незваными гостями. Для получения дополнительной информации см.:

    - INSECURE Security Tool (http://sectools.org)
    - FrSIRT Vulnerability Archive (http://www.frsirt.com/english)
    - Secunia Vulnerability Archive (http://secunia.com)
    - SecurityFocus Vulnerability Archive (http://www.securityfocus.com/bid)

Средства анализа уязвимости сети анализирует уязвимость таких сетевых ресурсов, как маршрутизаторы, брандмауэры и серверы.

Средство анализа уязвимости серверов анализирует такие уязвимости, как слабый пароль, слабая конфигурация и ошибка задания разрешения файла во внутренней системе. Средство анализа уязвимости серверов обеспечивает сравнительно более

точные результаты, чем средство анализа уязвимости сети, поскольку данный инструмент анализирует многие другие уязвимости во внутренней системе.

Средство анализа уязвимости в вебсети анализирует уязвимость веб-приложений, таких как: XSS и внедрение SQL-кода через сеть. Более подробную информацию можно найти в Проекте безопасности открытых веб-приложений: http://www.owasp.org/index.php/Top_10_2007.

Технология обнаружения

Технология обнаружения используется для выявления и отслеживания аномального состояния и проникновений в сеть или важные системы. Технология обнаружения включает в себя следующее:

1. Антивирусы – Антивирусное программное обеспечение представляет собой компьютерную программу для выявления, нейтрализации или устранения вредоносного кода, в том числе червей, фишинг-атак, руткитов (rootkit), «Троянских коней» и других вредоносных программ.[13]

2. Система обнаружения вторжений (СОВ) – СОВ собирает и анализирует информацию из различных областей компьютера или сети выявления возможных нарушений в системе безопасности. Функции обнаружения вторжений включают анализ аномальной активности и способность распознавать атакующие шаблоны.

3. Система предотвращения вторжения (СПВ) – предотвращение вторжения стремится определить потенциальные угрозы и среагировать на них прежде, чем они будут использоваться при атаках. СПВ контролирует сетевой трафик и принимает незамедлительные меры в отношении потенциальных угроз в соответствии с набором правил, установленных администратором сети. Например, СПВ может заблокировать трафик от подозрительного IP-адреса.[14]

Технология интеграции

Технологии интеграции объединяют важные функции для обеспечения информационной безопасности основных активов, такие как: прогнозирование, выявление и отслеживание вторжений. Технология интеграции включает в себя следующее:

1. Управление безопасностью предприятия (УБП) – система УБП управляет, контролирует и приводит в действие решения по информационной безопасности, как: СОВ и СПВ, основанные на последовательной политике. УБП используется в качестве стратегии для компенсации слабых сторон других решений, используя преимущества каждого решения для информационной безопасности и повышая эффективность информационной безопасности при осуществлении последовательной политики.

   УБП, которые искусственно могут управлять существующими технологиями безопасности, появились недавно из-за нехватки человеческих ресурсов по управлению технологиями безопасности, увеличения модернизированных нападений, таких как конвергенция методов нападения, и появления средств нападения, которые

13 Wikipedia, “Antivirus software,” Wikimedia Foundation, Inc., http://en.wikipedia.org/wiki/Antivirus_software.
14 SearchSecurity.com, “Intrusion prevention,” TechTarget, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1032147,00.html.

трудно обнаружить. С помощью УБП повысилась эффективность управления, и были приняты активные меры противодействия.

2. Управление рисками предприятия (УРП) – Система УРП помогает спрогнозировать все риски, относящиеся к организации, включая риски в областях за пределами информационной безопасности, и автоматически сформировать меры противодействия. Использование УРП для защиты информации требует определения точной цели применения управления рисками и проектирования для развития системы. Большинство организаций создает и оптимизирует свою собственную систему УРП через профессиональные консультационные агентства по информационной безопасности вместо того, чтобы делать это самим.

Вопросы для размышления

1. Перед какими угрозами информационной безопасности ваша организация уязвима? Почему?

2. Какие технологические решения по обеспечению информационной безопасности имеются в вашей организации?

3. Есть ли в вашей организации политика информационной безопасности, стратегия и руководящие принципы? Если да, то насколько они соответствуют тем угрозам, перед которыми уязвима ваша организация? Если нет, что вы могли бы порекомендовать в качестве политики, стратегии и руководящих принципов для обеспечения информационной безопасности вашей организации?

Проверьте себя

1. Почему важно проводить анализ тенденций угроз информационной безопасности?

2. Почему управление человеческими ресурсами является наиболее важным фактором в работе информационной безопасности? Какие существуют основные мероприятия в управлении человеческими ресурсами для информационной безопасности?

3. Объясните концепцию технологии безопасности «Глубокая оборона». Как она работает?

3. ДЕЯТЕЛЬНОСТЬ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задачи данного раздела:
- **Привести примеры деятельности различных стран по обеспечению информационной безопасности, которые будут служить ориентиром при разработке политики информационной безопасности;**
- **Рассмотреть значение международного сотрудничества в реализации политики информационной безопасности.**

3.1 Деятельность по обеспечению национальной информационной безопасности

Стратегия информационной безопасности США

После террористических атак 11 сентября 2001 года (9/11) США учредили Департамент по национальной безопасности с целью укрепления национальной безопасности не только от физических угроз, но также и против киберугроз. США осуществляют всеобъемлющую и эффективную деятельность по информационной безопасности через систему службы по информационной безопасности. Стратегия по обеспечению информационной безопасности включает Национальную стратегию безопасности, Национальную стратегию в области физической безопасности важнейших инфраструктур и ключевых объектов, а также Национальную стратегию по обеспечению безопасности киберпространства.

Национальная стратегия по обеспечению безопасности киберпространства[15] устанавливает видение кибербезопасности и защиту критической инфраструктуры и ресурсов. В ней определены конкретные цели и мероприятия по предотвращению кибератак против важных объектов инфраструктуры и активов. Существуют пять приоритетов, определенных в Национальной стратегии по обеспечению безопасности киберпространства:

- Национальная система реагирования по обеспечению безопасности киберпространства
- Национальная программа сокращения угрозы и уязвимости безопасности киберпространства
- Национальная программа обучения и информирования по обеспечению безопасности киберпространства
- Обеспечение безопасности киберпространства правительства
- Национальная безопасность и международное сотрудничество в области защиты киберпространства

15 The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, 2003), http://www.whitehouse.gov/pcipb.

Акт о дополнительных мерах по обеспечению кибербезопасности от 2002 года[16] (CSEA - Cyber Security Enhancement Act) включает в себя вторую главу закона о национальной безопасности. Он предусматривает среди прочего поправки к составлению нормативов для определенных компьютерных преступлений, разглашения информации в чрезвычайных ситуациях, исключения в случае честных намерений, запрет рекламы незаконных устройств в Интернете, а также защиту частной жизни.

Разглашение информации в чрезвычайных ситуациях: До 9/11 Акт о частной электронной связи (ECPA - Electronic Communications Privacy Act) запрещал поставщикам электронных услуг связи (например, Интернет-провайдерам) разглашать данные о пользовательских коммуникациях (например, голосовая почта, электронная почта и приложения). Разглашение информации в чрезвычайных ситуациях позволяет Интернет-провайдерам предоставлять содержание электронной почты или электронной связи правоохранительным органам без ордера согласно Акту о патриотизме США, принятому после 11 сентября 2001 года. Исключения из правил по обнародованию в случае чрезвычайной ситуации были закреплены в CSEA. Правительственные учреждения, получающие информацию с подозрительным содержанием, обязаны сообщить Генеральному прокурору дату раскрытия информации, вовлеченные стороны, раскрытую информацию и число обратившихся за данной информацией лиц, а также частоту коммуникаций в течение 90 дней после раскрытия.

Исключение в случае честных намерений: CSEA предусматривает освобождение от уголовных и гражданских наказаний в случае, если прослушивание запрашивается владельцем компьютера или оператором.

Запрет рекламы незаконных устройств в Интернете: ECPA запрещает изготовление, распространение, владение и онлайн-рекламу устройств перехвата проводной, устной и электронной информации. Электронные устройства слежения могут рекламироваться. Однако рекламодатель обязан знать содержание рекламы.

Усиление наказания за компьютерные нарушения: Согласно законодательному акту США о компьютерном мошенничестве и злоупотреблении преднамеренный доступ к компьютеру и причинение вреда без разрешения считается незаконным. До 9/11 любой человек, признанный виновным в этом преступлении, должен был быть приговорен к заключению не более чем на пять лет в случае первого преступления и не более чем на 10 лет в случае повторного правонарушения. После 9/11 наказание за такие нарушения было пересмотрено в виде лишения свободы не более чем на 10 лет при первом нарушении и не более чем на 20 лет при повторном преступлении. Дополнительные положения в CSEA предусматривают, что лицо, совершившее преступление, может быть приговорено к заключению не более чем на 20 лет, если преступник причинил или пытался причинить серьезное телесное повреждение; он/она может быть приговорен/а к пожизненному заключению, если он/она причиняет или пытается причинить смерть.

Освобождение от ответственности помощников: ECPA освобождает от уголовного наказания поставщиков услуг связи, которые помогают в перехвате информации или предоставляют информацию правоохранительным органам.

Акт о федеральном управлении информационной безопасностью (Federal Information Security Management Act , FISMA)[17] включает третью главу Акта об

16 Computer Crime and Intellectual Property Section, SEC. 225. *Cyber Security Enhancement Act of 2002* (Washington, D.C.: Department of Justice, 2002), http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm.

17 Office of Management and Budget, *Federal Information Security Management Act: 2004 Report to Congress* (Washington, D.C.: Executive Office of the President of the United States, 2005), http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf.

электронном правительстве от 2002 года. Данный закон защищает национальную сетевую инфраструктуру и призывает к активизации усилий по защите информационной безопасности всех граждан, агентства национальной безопасности и правоохранительные органы. Главными целями федерального управления информационной безопасностью являются: (1) обеспечение всеобъемлющей основы для повышения эффективности управления информационной безопасностью при эксплуатации и ресурсов; и (2) разработка надлежащего плана контроля и поддержки для защиты информации/информационных систем, а также обеспечение механизма для укрепления управления программ по информационной безопасности.

Стратегия по информационной безопасности Европейского Союза

В сообщении от мая 2006 года[18] Европейская комиссия описывает недавнюю стратегию по информационной безопасности Европейского союза (ЕС), состоящую из ряда взаимосвязанных мер с участием многих заинтересованных сторон. Эти меры включают в себя создание нормативно-правовой базы для электронных коммуникаций в 2002 году, объединение инициатив под названием «i2010» для создания Европейского информационного общества и учреждение в 2004 году Европейского агентства по сетевой и информационной безопасности (ENISA - European Network and Information Security Agency). Согласно сообщению, данные меры отражают трехаспектный подход к вопросам безопасности в информационном обществе, охватывающий определенные меры по сетевой и информационной безопасности (СИБ), нормативно-правовую базу для электронных коммуникаций (которая включает вопросы безопасности персональных данных) и борьбу с киберпреступностью.

Сообщение Европейской комиссии отмечает нападения на информационные системы, рост применения мобильных устройств, появление «окружающей разведки», а также повышение уровня информированности пользователей в качестве основных вопросов безопасности, которые Европейская комиссия стремится решать путем диалога, партнерства и расширения возможностей. Данные стратегии описаны в Сообщении следующим образом:

Диалог

Европейская комиссия предлагает ряд мер, направленных для установления открытого, содержательного и многостороннего диалога:

- Осуществление сопоставительного анализа для национальных политик, имеющих отношение к сетевой и информационной безопасности, чтобы помочь определить наиболее эффективные методы так, чтобы они могли затем быть применены на более широкой основе на всей территории ЕС. В частности, данный анализ выявит передовой опыт по повышению информированности малых и средних предприятий (МСП) и граждан об опасностях и проблемах, связанных с сетевой и информационной безопасностью;
- Структурированное многостороннее обсуждение того, как наилучшим образом использовать существующие нормативные документы. Данная дискуссия будет организована в рамках конференций и семинаров.

18 Europa, “Strategy for a secure information society (2006 communication),” European Commission, http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

Партнерство

Эффективная разработка политики требует четкого представления о характере задач, которые предстоит решать, а также надежных, обновленных статистических и экономических данных. Таким образом, Европейская комиссия будет просить ENISA о:

- формировании доверительного сотрудничества стран-членов и заинтересованных сторон с целью разработки соответствующей платформы для сбора данных;
- изучении возможности Европейской системы информационного обмена и оповещения в целях содействия эффективному реагированию на угрозы. Данная система будет включать многоязычный Европейский портал для предоставления специализированной информации об угрозах, рисках и предупреждениях.

Параллельно с этим Комиссия предложит странам-членам, частному сектору и научно-исследовательскому сообществу установить партнерские отношения в целях обеспечения доступности данных, имеющих отношение к индустрии безопасности в области ИКТ.

Расширение возможностей

Расширение прав и возможностей заинтересованных сторон является необходимым условием для развития их осведомленности о потребностях в области безопасности и рисков. В связи с этим странам-членам предлагается:

- Активно участвовать в осуществлении предложенного сопоставительного анализа национальных политик;
- В сотрудничестве с ENISA организовывать информационно-пропагандистские кампании о преимуществах внедрения эффективных технологий безопасности, передового опыта и поведения;
- Усилить внедрение электронных государственных услуг для продвижения передового опыта по обеспечению безопасности;
- Стимулировать развитие программ сетевой и информационной безопасности в качестве составной части учебных программ высших учебных заведений

Заинтересованным сторонам из частного сектора также предлагается взять инициативу по:

- Определению ответственности для производителей программного обеспечения и Интернет-провайдеров в отношении обеспечения соответствующих и проверяемых уровней безопасности;
- Содействию разнообразию, открытости, совместимости, удобству использования и конкуренции в качестве ключевых факторов для обеспечения безопасности, а также стимулированию внедрения повышающих безопасность продуктов и услуг для борьбы с кражами личных данных и другими нападениями, вторгающимися в частную жизнь;

- Распространению передового опыта по обеспечению безопасности для сетевых операторов, поставщиков услуг и МСП;
- Содействию обучающих программ в частном секторе для предоставления работникам знаний и навыков, необходимых для реализации практических методов по безопасности;
- Работе, направленной для обеспечения доступных схем сертификации по безопасности для продуктов, процессов и услуг, которые помогут в удовлетворении потребностей, характерных для ЕС;
- Привлечению страхового сектора в развитие средств и методов управления рисками

Источник: С сокращениями из Europa, «Strategy for a secure information society (2006 communication)», European Commission, http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

Конвенция Совета Европы о киберпреступности

В дополнение ко всему в 2001 году ЕС обнародовал Конвенцию Совета Европы о киберпреступности (КСЕК), которая «устанавливает руководящие принципы для всех правительств, желающих развивать законодательство по борьбе с киберпреступностью» и «служит основой для международного сотрудничества в этой области». Тридцать девять европейских стран, а также Канада, Япония, Южная Африка и США подписали данный договор. Это делает КСЕК, вступившую в силу в июле 2004 года, «единственным обязательным международным соглашением по данному вопросу, который осуществляется до настоящего времени».[19]

Европейское агентство по сетевой и информационной безопасности

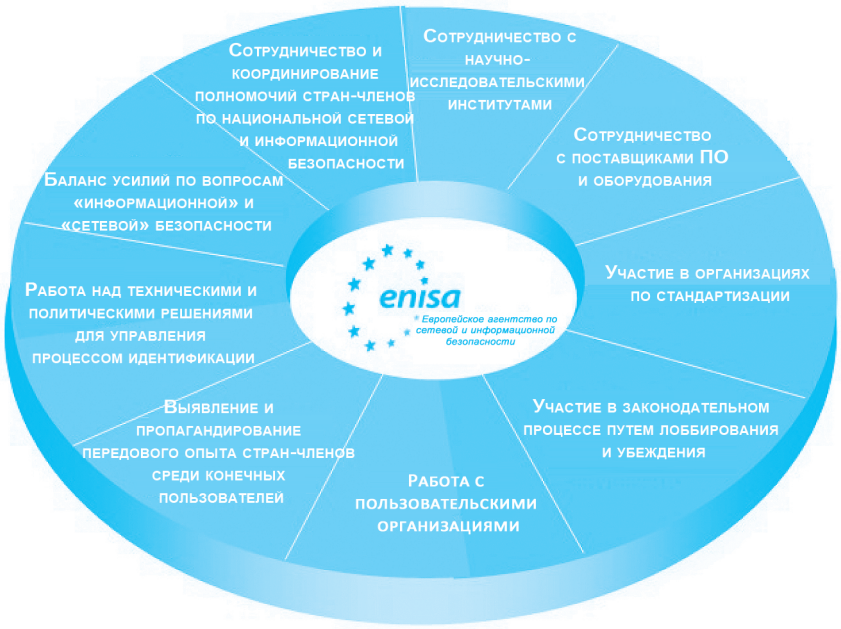
10 марта 2004 года Европейским парламентом и Советом ЕС было учреждено Европейское агентство по сетевой и информационной безопасности (European Network and Information Security Agency, ENISA), «чтобы способствовать укреплению сетевой и информационной безопасности в пределах ЕС и содействовать формированию культуры сетевой и информационной безопасности на благо граждан, потребителей, предприятий и организаций государственного сектора».

В концепции постоянной группы заинтересованных сторон (Permanent Stakeholders Group, PSG) для ENISA[20], сформулированной в мае 2006 года, ENISA видится в качестве центра передового опыта в области сетевой и информационной безопасности, форума для заинтересованных сторон в СИБ, а также движущей силы информированности по вопросам информационной безопасности всех граждан ЕС. С этой целью следующие долгосрочные меры для ENISA предусмотрены в концепции PSG (Рисунок 6):

19 Council of Europe, “Cybercrime: a threat to democracy, human rights and the rule of law,” http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.
20 Paul Dorey and Simon Perry, ed. *The PSG Vision for ENISA* (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

Рисунок 6. Долгосрочные меры для ENISA

(Источник: Paul Dorey and Simon Perry, ed. *The PSG Vision for ENISA* (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf)



1. **Сотрудничать и координировать полномочия стран-членов по национальной сетевой и информационной безопасности**

   В настоящее время сотрудничество между национальными агентствами очень слабое. Улучшить ситуацию возможно путем укрепления связей и расширения сотрудничества между национальными агентствами, в частности в области обмена передовым опытом ведущих агентств с только что образованными.

2. **Сотрудничать с научно-исследовательскими институтами**

   Целью ENISA должно быть направление фундаментальных исследований и целенаправленных технических разработок на то, чтобы сосредоточить внимание на областях, представляющих наибольшую пользу для управления фактическими рисками безопасности в реальных системах. ENISA не должно поддерживать сами программы исследований, а скорее работать над приведением в соответствие действующих процессов и приоритетов существующих программ.

3. **Сотрудничать с поставщиками программного обеспечения и оборудования**

   Поставщики программного обеспечения и аппаратных средств являются, по определению, конкурентами, и для них может быть трудным открыто договориться о скоординированных действиях. ENISA может обеспечить непредвзятое мнение и площадку для обсуждения чувствительных тем, сохраняя при этом необходимую чистоту в отношении антиконкурентного поведения.

В долгосрочной перспективе ENISA следует уделять больше внимания созданию надежных сетевых и информационных технологий, устойчивых к «червям» и другим проблемам, вместо того, чтобы продлевать нынешние инкрементные тенденции безопасности. Это может быть достигнуто развитием технологий для разработки правильных, безопасных и надежных архитектур и программного обеспечения.

4. **Участвовать в организациях по стандартизации**

   С целью выявления и пропаганды значимых инициатив ENISA должно отслеживать и контролировать темы, связанные с СИБ, в организациях по стандартизации, в том числе выполнение работ различных органов по сертификации и аккредитации по безопасности.

5. **Участвовать в законодательном процессе путем лоббирования и убеждения**

   ENISA должно работать над получением статуса доверенного консультанта для того, чтобы быть услышанным на ранних этапах процесса разработки и внесения предложений директив и других законопроектов в вопросах, связанных с СИБ.

6. **Работать с пользовательскими организациями**

   Зачастую организации пользователей не так широко представлены в законодательных органах и организациях по стандартизации, как поставщики. ENISA может предоставить группам конечных пользователей участие в работе над стандартами и возможность оказывать влияние на такие работы.

7. **Выявлять и пропагандировать передовой опыт стран-членов среди конечных пользователей**

   ENISA должно не только защищать бизнес-интересы, но также укреплять доверие конечных пользователей в использовании Интернета и цифровых средств массовой информации.

8. **Работать над техническими и политическими решениями для управления процессом идентификации**

   Отсутствие доверия в Интернете представляет собой основное препятствие на пути развития крупномасштабного электронного бизнеса, ориентированного на потребителя. Способность точно проверить личность владельца сайта, электронного адреса или какой-либо онлайн-услуги будет огромным шагом на пути к обновлению и повышению доверия обычного пользователя в Интернете. Технические решения в этой области должны быть найдены через процессы, движущие данную индустрию, но ENISA может работать над политикой аутентификации субъектов в сети в масштабах Европейского союза.

9. Сбалансировать усилия по вопросам «информационной» и «сетевой» безопасности

ENISA должно поддерживать связь с крупнейшими поставщиками сетевых и Интернет-услуг (ISP/NSP) для организации помощи по определению передового опыта, полезного для бизнеса и потребителей в Европе. Это важно, потому что ISP/NSP могут играть ключевую роль в повышении безопасности в Интернете в целом. Существующие сотрудничество и координация действий, которые предпринимают поставщики Интернет-услуг, недостаточны в настоящее время.

Источник: С сокращениями из Paul Dorey and Simon Perry, ed. *The PSG Vision for ENISA* (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

Стратегия информационной безопасности Республики Корея

Несмотря на то, что Республика Корея является одной из самых передовых стран мира в области интернет-технологий, она лишь недавно рассмотрела вопрос о необходимости обеспечения информационной безопасности. В 2004 году правительство Кореи через Министерство информации и связи (МИС) опубликовало средне- и долгосрочный План действий («Дорожная карта») по информационной безопасности с целью создания платформы по информационной безопасности для обеспечения безопасной среды связи для широкополосной единой инфраструктуры (Broadband Convergence Network) и разработки технологии безопасности против незаконного копирования мобильного оборудования следующего поколения. МИС также попыталось ввести систему оценки воздействия на персональные данные (Privacy Impact Assessment, PIA) и создать средства для сертификации взрослого населения, используя регистрационные номера резидентов. Кроме того, Республика Корея подписала Соглашение между Сеулом и Мельбурном по построению сотрудничества между странами Азиатско-Тихоокеанского региона для борьбы со спамом путем внедрения системы контроля за спамом, технологического реагирования, обучения пользователей и повышения осведомленности, усовершенствования частного и государственного сотрудничества по обмену информацией между странами, а также человеческими ресурсами.

Основные цели «Дорожной карты» по информационной безопасности следующие: (1) обеспечить безопасность сетевых инфраструктур; (2) обеспечить надежность новых ИТ-услуг и оборудования; и (3) содействовать построению основы информационной безопасности в Республике Корея. Реализация «Дорожной карты» предполагает четырехлетнее бюджетное распределение 247,89 млрд. долл. США (43 млрд. долл. США в 2005 году, 55,5 млрд. долл. США в 2006 году, и 80,1 млрд. долл. США в 2008 году).

Обеспечение безопасности сетевой инфраструктуры: В соответствии с «Дорожной картой», безопасность сетевых инфраструктур должна быть обеспечена путем создания платформы по информационной безопасности для интеграции и взаимосвязи различных разнородных компьютерных сетей; создания управления безопасностью системы доменных имен следующего поколения; а также развития механизма разделения сети для предотвращения повреждений в среде широкополосной единой инфраструктуры и их распространения в частных сетях, и наоборот.

Обеспечение надежности новых ИТ-услуг и устройств: Для эффективного предотвращения нарушений информационной безопасности в новых ИТ-услугах будет разработана модель оценки воздействия на информационную безопасность, которая может оценить административные, технические и физические угрозы и уязвимости.

Будет выполнена процедура сертификации для оценки уровней информационной безопасности. Для следующего поколения ИТ-услуг система сертификации будет модернизирована так, чтобы включать сертификацию людей, органов власти, учета транзакций и т.п.

Кроме того, был сформулирован план развития технологий по информационной безопасности, который включает в себя соответствующую технологию предоставления прав доступа для домашних сетей, пограничную технологию идентификации для предотвращения незаконного вторжения, технологию безопасности для обслуживающих роботов следующего поколения и технологию безопасности информационного содержания следующего поколения.

Создание основы информационной безопасности: «Дорожная карта» по информационной безопасности Кореи содержит положения по совершенствованию регулирования в соответствии с требованиями меняющейся информационно-коммуникационной среды для подготовки к будущим угрозам. Во-первых, должен быть усовершенствован Центр службы реагирования на Интернет-инциденты, чтобы справляться со сложными и высокоразвитыми формами случаев Интернет-вторжений. Должны быть улучшены отечественные и зарубежные системы сотрудничества по информационной безопасности и оказана поддержка для систем со слабой информационной безопасностью. Во-вторых, должны быть созданы соответствующие технологии, а также законы о защите частной жизни. Также должен заработать Центр службы реагирования на спам. В-третьих, для удовлетворения потребностей всепроникающей глобальной среды должны быть улучшены существующие законы по информационной безопасности. Кроме того, с помощью информационных кампаний и программ обучения специалистов должно быть обеспечено понимание важности информационной безопасности.

Стратегия информационной безопасности Японии[21]

В соответствии со своей целью стать «страной, передовой в вопросах информационной безопасности»,[22] Япония изложила подробный список целей, основных принципов и проектов в области информационной безопасности. Совет по политике информационной безопасности и Национальный центр по информационной безопасности (НЦИБ) являются основными организациями, отвечающими за всю работу, связанную с информационной безопасностью в стране. В области научных исследований по киберугрозам был учрежден Центр обеспечения киберчистоты (Cyber Clean Center) для анализа особенностей ботов и формулирования эффективных и безопасных методов реагирования.

Стратегия информационной безопасности Японии состоит из двух частей: (1) Первая национальная стратегия в области информационной безопасности, которая применяется в целом; и (2) Безопасная Япония ГГГГ. Первая национальная стратегия в области информационной безопасности признает необходимость для всех «субъектов» ИТ-общества «участвовать в создании среды для безопасного использования ИТ».[23]

21 This section is drawn from NISC, *Japanese Government's Efforts to Address Information Security Issue* (November 2007), http://www.nisc.go.jp/eng/.
22 Information Security Policy Council, *The First National Strategy on Information Security* (2 February 2006), 5. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.
23 Там же, 11.

Стратегия признает субъекты, «которые фактически принимают и осуществляют меры в качестве одного из компонентов ИТ-общества».[23] Такие «субъекты» делятся на четыре категории: центральные и местные органы управления, критические инфраструктуры, бизнес-структуры и физические лица. Каждый из них обязан определить свою собственную роль и планы и управлять ими (Таблица 4).

Таблица 4. Роли и планы каждой категории в соответствии с Первой национальной стратегией в области информационной безопасности

Категория	Роли	Планы
Центральные и местные органы управления	Предоставление передового опыта для измерения показателей информационной безопасности	Стандарты для измерения
Критические инфраструктуры	Обеспечение стабильного оказания услуг в качестве основы социальной жизни и экономической деятельности людей	План действий по критическим инфраструктурам
Бизнес-структуры	Внедрение мер по обеспечению информационной безопасности, защищающих деятельность рынка	Меры, принимаемые министерствами и агентствами
Физические лица	Повышение осведомленности в качестве основного игрока ИТ-общества	Меры, принимаемые министерствами и агентствами

Источник: НСИБ, Усилия правительства Японии по обеспечению информационной безопасности (ноябрь 2007 г.), http://www.nisc.go.jp/eng/.

Практическими методами из Первой национальной стратегии в области информационной безопасности являются следующие:

- Содействие развитию технологий по информационной безопасности – Разработка технологий, предназначенных для использования правительством, и содействие развитию технологий для решения «Великого вызова» основных инновационных технологий в долгосрочной перспективе;
- Содействие развитию международного взаимодействия и сотрудничества – Участие в создании международной платформы по информационной безопасности и его обеспечения, и осуществление международных вкладов под лидерством Японии;
- Развитие человеческих ресурсов – Развитие человеческих ресурсов с практическими навыками, талантами и всесторонними способностями, а также организация системы квалификации по информационной безопасности;
- Борьба с преступностью и меры по защите/исправлению прав и интересов – Укрепление контроля за киберпреступностью и разработка соответствующей правовой базы, а также развитие технологий для усовершенствования безопасности в киберпространстве.

Безопасная Япония ГГГГ представляет собой ежегодный план по информационной безопасности. «Безопасная Япония 2007» включает 159 мер по обеспечению информационной безопасности и руководство по разработке документов по 24 приоритетам на 2007 год. Они могут быть вкратце изложены следующим образом:

- Повышение мер информационной безопасности для центральных государственных учреждений;
- Распространение мер как для организаций, которые отстают в принятии мер по обеспечению информационной безопасности, так и для широкой публики;
- Интенсивные усилия по укреплению основ информационной безопасности.

Вопросы для размышления

1. В чем сходства и отличия деятельности по обеспечению информационной безопасности в вашей стране с теми, что описаны выше?

2. Существуют ли виды деятельности по информационной безопасности, предпринимаемые в странах, упомянутых в этом разделе, которые не применимы или имеют отношение к вашей стране? Если да, то какие и почему они не применимы или уместны?

3.2 Международная деятельность по обеспечению информационной безопасности

Деятельность ООН по обеспечению информационной безопасности

На **Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО),**[24] организованной под эгидой ООН, были приняты Декларация принципов и План действий для эффективного роста информационного общества и устранения «информационного разрыва». План действий определяет следующие направления деятельности:

- Роль органов государственного управления и всех заинтересованных сторон в содействии применению ИКТ в целях развития
- Информационная и коммуникационная инфраструктура в качестве необходимого фундамента для всего информационного общества
- Доступ к информации и знаниям
- Наращивание потенциала
- Укрепление доверия и безопасности при использовании ИКТ
- Создание благоприятной среды
- Применение ИКТ во всех аспектах жизни
- Культурное разнообразие и самобытность, языковое разнообразие и местное информационное содержание
- Средства массовой информации
- Этические аспекты информационного общества
- Международное и региональное сотрудничество[25]

24 World Summit on the Information Society, “Basic Information: About WSIS,” http://www.itu.int/wsis/basic/about.html.
25 World Summit on the Information Society, *Plan of Action* (12 December 2003), http://www.itu.int/wsis/docs/geneva/official/poa.html.

Форум по вопросам управления Интернетом (ФУИ)[26] является вспомогательной организацией ООН по вопросам управления использованием Интернета. Он был учреждён после второго этапа ВВУИО в Тунисе для определения и решения вопросов, связанных с управлением Интернетом. Основной темой второго форума ФУИ, проведенного в Рио-де-Жанейро с 12 по 15 ноября 2007 году, были проблемы информационной безопасности, такие как: кибертерроризм, киберпреступность и безопасность детей в Интернете.

Деятельность ОЭСР по обеспечению информационной безопасности[27]

Организация экономического сотрудничества и развития (ОЭСР) является уникальным форумом, где правительства 30 стран с рыночной демократией взаимодействуют совместно с деловыми кругами и гражданским обществом в целях решения экономических, социальных, экологических проблем и вопросов управления, стоящих перед глобализацией мировой экономики. На основе мандата, полученного от Комитета ОЭСР по информационной, компьютерной и коммуникационной политике, свою деятельность осуществляет Рабочая группа по информационной безопасности и неприкосновенности частной жизни (Working Party on Information Security and Privacy, WPISP) для обеспечения анализа воздействия ИКТ на информационную безопасность и неприкосновенность частной жизни, а также разработки политических рекомендации на основе консенсуса по укреплению доверия в экономической деятельности с помощью Интернета.

Деятельность WPISP в области информационной безопасности: В 2002 году ОЭСР опубликовала «Директивы по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности»[28] для содействия «обеспечению безопасности при разработке информационных систем и сетей, а также принятие новой модели мышления и поведения при использовании информационных систем и сетей и при взаимодействии с ними».[29]

Для обмена передовым опытом и практикой в области информационной безопасности были проведены: в 2003 году – Глобальный форум по безопасности информационных систем и сетей, и в 2005 году – Семинар ОЭСР-АТЭС (Азиатско-Тихоокеанское Экономическое Сообщество) по проблемам безопасности информационных систем и сетей.

Деятельность WPISP по проблемам неприкосновенности частной жизни: «Директивы ОЭСР, регламентирующие обеспечение неприкосновенности частной жизни и защиту трансграничных потоков данных о частных лицах», принятые в 1980 году, представляют собой международный консенсус в отношении обработки персональной информации в государственных и частных секторах. «Неприкосновенность частной жизни в онлайне: Руководство ОЭСР, регламентирующая политику и практику», принятое в 2002 году, основное внимание уделяет технологиям, повышающим неприкосновенность частной жизни, политике неприкосновенности в онлайне, осуществлении и восстановлении и т.п. относительно электронной коммерции. В настоящее время WPISP работает над сотрудничеством по осуществлению правосудия в области неприкосновенности частной жизни.

Другие направления деятельности: В 1998 году ОЭСР выпустила «Директивы, регламентирующие политику в сфере криптографии» и приняла Декларацию об

26 Internet Governance Forum, http://www.intgovforum.org.
27 This section is drawn from WPISP, “Working Party on Information Security and Privacy” (May 2007).
28 OECD, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (Paris: OECD, 2002), http://www.oecd.org/dataoecd/16/22/15582260.pdf.
29 Там же, 8.

аутентификации в электронной коммерции, принятую на уровне министров в Оттаве. В период с 2002 по 2003 гг. проводился «Обзор правовых и политических основ для обеспечения услуг по электронной аутентификации и электронных подписей в странах-членах ОЭСР». В 2005 году было издано «Использование системы аутентификации на границах стран ОЭСР».

В 2004 г. были написаны «Технологии, основанные на биометрических методах», и в 2005 году была сформирована специальная группа по борьбе со спамом. Другие работы, проводимые в настоящее время, имеют отношение к управлению цифровой идентификацией, вредоносным ПО, радиочастотной идентификации (RFID), датчикам и сетям, а также общей базовой основе по обеспечению информационной безопасности и неприкосновенности частной жизни.

Деятельность АТЭС по обеспечению информационной безопасности[30]

Азиатско-Тихоокеанское экономическое сообщество (АТЭС) осуществляет деятельность по обеспечению информационной безопасности в Азиатско-Тихоокеанском регионе через рабочую группу по телекоммуникациям и информации (ТЕЛ), которая состоит из трех исполнительных комитетов: исполнительный комитет по либерализации, исполнительный комитет по развитию ИКТ и исполнительный комитет по безопасности и процветанию.

Особенно с тех пор, как в июне 2005 г. прошло 6-ое заседание АТЭС на уровне министров по телекоммуникационной и информационной промышленности в Лиме, Перу, исполнительный комитет по безопасности и процветанию активизировал дискуссии по проблемам кибербезопасности и киберпреступности. Стратегия АТЭС по проблемам кибербезопасности, которая включает в себя вопросы усиления доверия потребителей в использовании электронной коммерции, служит для объединения усилий различных стран. Данные усилия включают в себя принятие и осуществление законов по вопросам кибербезопасности, которые соответствуют Резолюции 55/63[31] Генеральной Ассамблеи ООН и Конвенции по киберпреступности.[32] Инициатива TEL по законодательству, рассматривающему проблемы киберпреступности, и Проект усиления потенциала по правоприменению будут поддерживать институты по осуществлению новых законов.

Члены АТЭС также совместно работают над реализацией службы реагирования на компьютерные инциденты (CERT) в качестве защитной системы раннего предупреждения против атак в киберпространстве. Республика Корея обеспечивает подготовку кадров для развивающихся стран-членов, а также руководящие принципы по созданию и организации работы CERT.

Защита МСП и домашних пользователей от киберугроз и вирусов считается приоритетной, и с этой целью разрабатываются множество инструментариев. Предоставляется информация о том, как безопасно использовать Интернет, а также по проблемам безопасности, имеющим отношение к беспроводным технологиям и обмену электронной почтой.

Снижение преступного неправильного использования информации через информационный обмен, разработку процедур и законов о взаимопомощи и другие меры

30 This section is drawn from APEC, "Telecommunications and Information Working Group," http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

31 'Combating the criminal misuse of information', which recognizes that one of the implications of technological advances is increased criminal activity in the virtual world.

32 An Agreement undertaken in Budapest that aims to uphold the integrity of computer systems by considering as criminal acts any action that violates said integrity. See http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

защиты бизнеса и граждан продолжают оставаться приоритетными направлениями для рабочей группы Азиатско-Тихоокеанского экономического сообщества по телекоммуникациям и информации (APECTEL). Как часть своей программы по проблемам безопасности, APECTEL утвердил в 2007 году «Директиву по политическим и техническим методам борьбы с ботнет» и провел семинар по проблемам безопасности в киберпространстве и критической информационной инфраструктуры.

Деятельность МСЭ по обеспечению информационной безопасности[33]

МСЭ является ведущим агентством ООН по вопросам ИКТ. В МСЭ, расположенном в Женеве, Швейцария, входят 191 государств-членов и свыше 700 членов секторов и ассоциированных членов.

Роль МСЭ в содействии мировой коммуникации охватывает три основных сектора. Сектор радиосвязи (МСЭ-Р) сосредоточен на управлении спектром международных радиочастот и ресурсами спутниковых орбит. Сектор стандартизации (МСЭ-Т) основное внимание уделяет стандартизации информационно-коммуникационных сетей и услуг. Сектор Развития (МСЭ-Д) был создан для помощи по распространению равного, устойчивого и приемлемого доступа к ИКТ в качестве средства стимулирования более широкого социально-экономического развития. МСЭ также организует мероприятия TELECOM и является ведущим организационным агентством ВВУИО.

В области безопасности в киберпространстве основными инициативами МСЭ являются «Направление деятельности С.5» ВВУИО, глобальная программа по кибербезопасности МСЭ, и шлюз кибербезопасности (Cybersecurity Gateway) МСЭ.

Главные пункты «Направлений деятельности С.5» ВВУИО:

- Защита критической информационной инфраструктуры (CIIP);
- Продвижение глобальной культуры кибербезопасности;
- Гармонизация национальных нормативно-правовых подходов, международной правовой координации и их правоприменение;
- Противодействие спаму;
- Развитие потенциала по наблюдению, оповещению и реагированию на инциденты;
- Обмен информацией о национальных подходах, передовом опыте и руководящих принципах;
- Защита неприкосновенности частной жизни, данных и потребителей.

Глобальная программа по кибербезопасности (ГПК) МСЭ является основой МСЭ для международного сотрудничества, направленного на предложение решений по укреплению доверия и безопасности в условиях информационного общества. ГПК основывается на пяти стратегических принципах: правовая база, технические меры, организационные структуры, наращивание потенциала и международное сотрудничество. Стратегии разработаны для достижения следующих целей:

- Разработка модельного законодательства по борьбе с киберпреступностью, применимого в глобальном масштабе и совместимого с существующими национальными и региональными мерами законодательного характера;
- Создание национальных и региональных организационных структур и политики в области борьбы с киберпреступностью;

33 This section is drawn from ITU, “About ITU,” http://www.itu.int/net/about/index.aspx.

- Определение приемлемых на глобальном уровне минимальных критериев безопасности и схем аккредитации для программных приложений и систем;
- Создание глобальной базовой структуры для наблюдения, оповещения и реагирования на инциденты в целях обеспечения трансграничной координации инициатив;
- Создание и утверждение общей и универсальной системы цифровой идентификации, а также необходимых организационных структур в целях обеспечения признания цифровых удостоверений личности без учета географических границ;
- Разработка глобальной стратегии в целях содействия созданию человеческого и институционального потенциала для расширения знаний и ноу-хау в различных секторах и во всех вышеупомянутых областях;
- Консультирование по созданию потенциальной основы для глобальной многосторонней стратегии в целях налаживания международного сотрудничества, диалога и координации деятельности во всех вышеупомянутых областях.

Шлюз кибербезопасности МСЭ направлен на предоставление простых в использовании информационных ресурсов для инициатив, которые имеют отношение к национальной и международной кибербезопасности. Он доступен для граждан, правительств, деловых кругов и международных организаций. Услуги, оказанные посредством Шлюза, включают информационный обмен, наблюдение и оповещение, законы и законодательство, конфиденциальность и защиту, а также отраслевые стандарты и решения.

МСЭ-Д также контролирует программу работ по кибербезопасности МСЭ, которая была создана для оказания помощи странам по развитию технологий на высоком уровне безопасности в киберпространстве. Она обеспечивает содействие в следующем:

- Создание национальных стратегий и возможностей для обеспечения кибербезопасности и CIIP
- Создание соответствующего законодательства о киберпреступлениях и механизмов правоприменения
- Создание системы наблюдения, оповещения и реагирования на инциденты
- Противодействие спаму и другим подобным угрозам
- Уменьшение разрыва стандартизации, имеющей отношение к безопасности систем, между развивающимися и развитыми странами
- Создание Директивы МСЭ по кибербезопасности/CIIP, базы контактных данных и именного указателя
- Создание показателей по проблемам кибербезопасности
- Укрепление регионального сотрудничества
- Информационный обмен и поддержка Шлюза кибербезопасности МСЭ
- Информационно-просветительская работа и поощрение связанных видов деятельности

Другие виды деятельности МСЭ-Д, связанные с кибербезопасностью: совместные мероприятия с организацией StopSpamAlliance.org; деятельность по усилению регионального потенциала в области законодательства о киберпреступлениях и правоприменения; развитие и распространение инструментария для уменьшения воздействия ботнет;[34] публикации на тему кибербезопасности/киберпреступности;[35] набор средств в качестве модели для законодательства по киберпреступности для развивающихся стран и инструментарий для самооценки системы национальной кибербезопасности.[36]

34 Suresh Ramasubramanian and Robert Shaw, “ITU Botnet Mitigation Project: Background and Approach” (ITU presentation, September 2007), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf.
35 ITU-D Applications and Cybersecurity Division, “Publications,” ITU, http://www.itu.int/ITU-D/cyb/publications/.
36 ITU-D Applications and Cybersecurity Division, “ITU National Cybersecurity / CIIP Self-Assessment Tool,” ITU, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Деятельность ISO/IEC по обеспечению информационной безопасности

Система управления информационной безопасностью (СУИБ) является, как следует из названия, системой для управления информационной безопасностью. Она состоит из процессов и систем для обеспечения конфиденциальности, целостности и доступности информационных ресурсов при одновременном сведении к минимуму рисков безопасности. Сертификация СУИБ становится все более популярной во всем мире, 2005 год стал поворотным моментом в истории стандартизированной на международном уровне СУИБ благодаря появлению на свет двух документов: IS 27001, который устанавливает требования для учреждения СУИБ, и IS 17799: 2000, опубликованного как IS 17799:2005, который предусматривает основные средства контроля для осуществления СУИБ.

Де-факто стандартом СУИБ был BS 7799, который был впервые разработан Британским институтом стандартов (BSI) в 1995 году как свод правил для управления информационной безопасностью. Поскольку разработанная спецификация требований основывалась на этом стандарте, в 1998 году «свод правил для управления информационной безопасностью» был изменен на Часть 1, а спецификация требований стала Частью 2. Часть 1 описывает средства контроля для управления информационной безопасностью, в то время как Часть 2 излагает требования для создания СУИБ и описывает процесс информационной безопасности (цикл «планирование-выполнение–проверка–корректировка») для непрерывного усовершенствования базы по управлению рисками.

Часть 1 была утверждена в качестве международного стандарта IS 17799 рабочей группой технического комитета ISO/IEC JTC 1/SC27 WG1 в 2000 году. С тех пор стандарт IS 17799 был пересмотрен (поступило свыше 2000 комментариев) и исправлен, и окончательная версия была добавлена к международному стандарту в ноябре 2005 года. IS 17799:2000 содержит 126 контрольных списков с 10 контрольными областями управления. Стандарт IS 17799, пересмотренный в 2005 году, охватывает 11 административных контрольных доменов и 133 области контроля.

Часть 2 стандарта BS 7799, созданная в 1999 году, использовалась в качестве стандарта для сертификации СУИБ. Она была пересмотрена в сентябре 2002 года на приведение наряду с другими в соответствие с ISO 9001 и ISO 14001. Международная организация по стандартизации ISO приняла BS7799 Часть 2: 2002 на основе ускоренного метода в связи с просьбами для международной стандартизированной СУИБ и зарегистрировала ее в качестве международного стандарта ISO27001, пересмотрев ее немного в течение короткого времени. Выполненные известные изменения включают добавление содержания по поводу эффективности и поправки в приложении.

Поскольку эти два важных документа, относящиеся к СУИБ, были стандартизированы на международном уровне, семейство международных стандартов по безопасности появилась под серийной нумерацией 27000, что является идентичным другим системам управления (управление качеством: серия 9000, экологическое управление: серия 14000). IS 27001, пересмотренная версия IS 17799: 2005, содержит требования для создания СУИБ, и IS 17799: 2005, который включает основные области контроля для внедрения СУИБ, был изменен на IS 27002 в 2007 году. Руководство по внедрению СУИБ, стандарт для управления рисками информационной безопасности, и система управления измерениями и параметрами информационной безопасности, разработанные техническим комитетом JTC1 SC27, содержатся в серии 27000.

Рисунок 7 показывает группу стандартов, относящихся к СУИБ. Деятельность по сертификации СУИБ набирает обороты, и ожидается, что стандарты или руководящие принципы СУИБ, соответствующие определенным отраслям промышленности, разрабатываются, основываясь на СУИБ для общепринятых систем. В качестве примера можно привести усилия для разработки руководящих принципов СУИБ, отражающих особенности индустрии коммуникаций.

Рисунок 7. Группа 27000 ISO/IEC

(ANSIL, «Дорожная карта» ISO/IEC 2700x, ISMS, Forum Eurosec 2007, http://www.ansil.eu/files/pres-eurosec2007-23052007.pdf)

Вопросы для размышления

Какие виды деятельности по обеспечению информационной безопасности, возглавляемые международными организациями, были приняты или принимаются в вашей стране? Как они осуществляются?

Проверьте себя

1. В чем сходство между мероприятиями по обеспечению информационной безопасности, предпринимаемыми в странах, указанных в данном разделе? В чем их отличия?

2. Каковы приоритеты международных организаций, включенных в данный раздел, относительно обеспечения информационной безопасности?

4. МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задачей данного раздела является описание административной, физической и технической методологий обеспечения информационной безопасности, используемых на международном уровне.

4.1 Методология обеспечения информационной безопасности

Методология обеспечения информационной безопасности призвана свести к минимуму ущерб и поддержание непрерывности бизнес-процессов с учетом всех возможных уязвимостей и угроз информационным ресурсам. Для обеспечения непрерывности бизнес-процессов методология информационной безопасности направлена на обеспечение конфиденциальности, целостности и доступности внутренних информационных ресурсов. Для этого применяются методы и области контроля оценки степени риска. По сути, необходим хороший план, который охватывает административные, физические и технические аспекты обеспечения информационной безопасности.

Административный аспект

Для многих СУИБ приоритетным является административный аспект. В большинстве случаев используется стандарт ISO/IEC27001.

ISO/IEC27001, международный стандарт СУИБ, основывается на стандарте BS7799, который был разработан Британским институтом стандартов (BSI). BS7799 определяет требования для внедрения и управления СУИБ и общие стандарты, применимые к стандартам безопасности различных организаций и эффективному управлению безопасностью. Часть 1 стандарта BS7799 описывает необходимые действия по обеспечению безопасности, основанные на передовом опыте по обеспечению безопасности в организациях. Часть 2, которая стала в настоящий момент стандартом ISO/IEC27001, предлагает минимальные требования, необходимые для работы СУИБ и оценки деятельности по обеспечению безопасности.

Деятельность по обеспечению безопасности в стандарте ISO/IEC27001 состоит из 133 областей контроля и 11 доменов (Таблица 5).

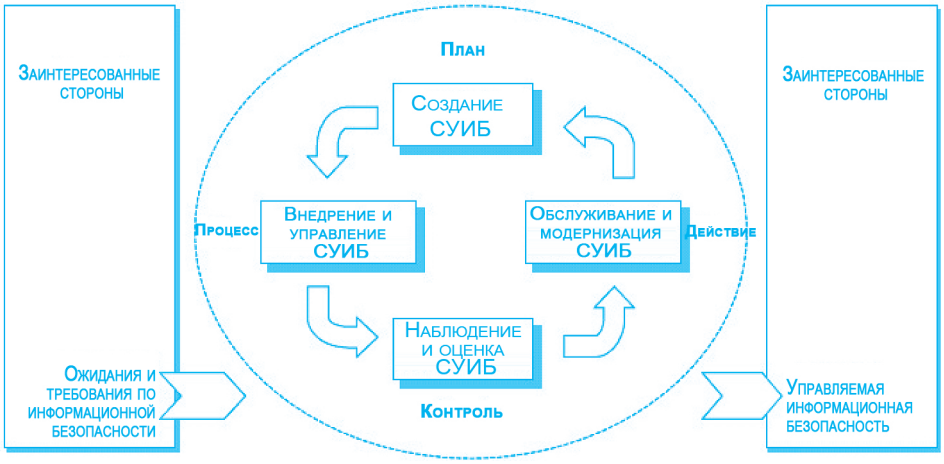
Таблица 5. Области контроля в ISO/IEC27001

Домены	Наименование
A5.	Политика безопасности
A6.	Организация системы информационной безопасности
A7.	Управление ресурсами
A8.	Безопасность человеческих ресурсов
A9.	Физическая безопасность и безопасность окружающей среды
A10.	Физическая безопасность и безопасность окружающей среды
A11.	Контроль доступа
A12.	Приобретение, развитие и эксплуатация информационных систем
A13.	Управление инцидентами информационной безопасности
A14.	Управление непрерывностью бизнес-процессов
A15.	Соответствие

Стандарт ISO/IEC27001 применяет модель процесса «Планирование–Выполнение–Проверка–Корректировка», которая применяется для структуризации всех процессов СУИБ. В ISO/IEC27001 все доказательства исполнения оценки СУИБ должны документироваться; в целях сертификации каждые шесть месяцев должен проводиться внешний аудит; а весь процесс необходимо повторять каждые три года с целью непрерывного управления СУИБ.

Рисунок 8. Модель процесса «Планирование–Выполнение–Проверка–Корректировка», применяемая к процессам СУИБ

(Источник: ISO/IEC JTC 1/SC 27)



Области контроля безопасности должны быть запланированы с учетом требований безопасности. Все человеческие ресурсы, включая поставщиков, подрядчиков, заказчиков и привлеченных специалистов, должны участвовать в этих мероприятиях. Установление требований безопасности основывается на следующих трех факторах:

- Оценка степени риска
- Юридические требования и условия контракта
- Информационные процессы для управления организацией

Анализ расхождения относится к процессу измерения текущего уровня обеспечения информационной безопасности и определения будущего направления развития информационной безопасности. Результат анализа расхождения составляется из ответов владельцев ресурсов на 133 области контроля и 11 доменов. Как только недостающие места будут выявлены в ходе анализа расхождения, на каждое такое место могут быть установлены соответствующие области контроля.

Оценка степени риска делится на оценку стоимости активов и оценку угроз и уязвимости. Оценка стоимости активов – это количественная оценка информационных ресурсов. Оценка угроз касается классификации угроз конфиденциальности, целостности и доступности информации. Нижеприведенный пример показывает вычисления, участвующие в оценке степени риска.

Наименование активов	Стоимость активов	Угроза			Уязвимость			Риск		
		C	I	A	C	I	A	C	I	A
Актив #1	2	3	3	1	3	1	1	8	6	5

- Стоимость активов + Угроза + Уязвимость = Риск
- Конфиденциальность: Стоимость активов(2) + Угроза(3) + Уязвимость(3) = Риск (8)
- Целостность: Стоимость активов(2) + Угроза(3) + Уязвимость(1) = Риск(6)
- Доступность: Стоимость активов(2) + Угроза(1) + Уязвимость(1) = Риск(5)

Применение областей контроля: Каждое значение риска будет отличаться в зависимости от результатов оценки степени риска. Необходимы решения для применения соответствующих областей контроля к активам, оцененным по-разному. Риски должны быть разделены на допустимые и недопустимые в зависимости от критерия «Степень уверенности». Области контроля должны быть применены к информационным ресурсам с недопустимым риском. Применяемые области контроля основаны на стандартах ISO/IEC, но более эффективным является применение областей контроля в зависимости от действительного состояния организации.

У каждой страны есть своя организация по сертификации ISO/IEC27001. В таблице 6 перечисляются количества сертификатов по странам.

Таблица 6. Число сертификатов по странам

Япония	2863*	Нидерланды	11	Болгария	2
Индия	433	Сингапур	11	Канада	2
Соединенное Королевство	368	Филиппины	10	Гибралтар	2
Тайвань	202	Саудовская Аравия	10	Остров Мэн	2
Китай	174	Пакистан	10	Марокко	2
Германия	108	Российская Федерация	10	Оман	2
США	82	Франция	9	Катар	2
Венгрия	74	Колумбия	7	Йемен	2
Республика Корея	71	Словения	7	Армения	1
Чешская Республика	66	Швеция	7	Бангладеш	1
Италия	54	Словакия	6	Бельгия	1
Гонконг	38	Хорватия	5	Египет	1
Польша	36	Греция	5	Иран	1
Австралия	28	Южная Африка	5	Казахстан	1
Австрия	26	Бахрейн	4	Кыргызстан	1
Ирландия	26	Индонезия	4	Ливия	1
Малайзия	26	Кувейт	4	Литва	1
Испания	26	Норвегия	4	Люксембург	1
Бразилия	20	Шри-Ланка	4	Македония	1
Мексика	20	Швейцария	4	Молдова	1
Тайланд	17	Чили	3	Новая Зеландия	1
Румыния	16	Макао	3	Украина	1
Турция	15	Перу	3	Уругвай	1
ОАЭ	14	Португалия	3	Относительная сумма	4997
Исландия	11	Вьетнам	3	**Абсолютная сумма**	**4987**

Примечание: Число сертификатов по странам приводится по состоянию на 21 декабря 2008 г.
Источник: International Register of ISMS Certificates, «Number of Certificates per Country», ISMS International User Group Ltd., http://www.iso27001certificates.com.

Физический аспект

В настоящее время не существует никакой международной системы управления физической информационной безопасностью. FEMA 426[37] (Федеральное агентство по чрезвычайным ситуациям США), которое является стандартом для физической СУИБ в Соединенных Штатах и используется многими странами в качестве методологии, будет рассмотрена подробнее.

37 FEMA, “FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings,” http://www.fema.gov/plan/prevent/rms/rmsp426.

FEMA 426 содержит руководящие принципы для защиты зданий от террористических атак. Данное руководство направлено на «создание научного сообщества архитекторов и инженеров для уменьшения физического повреждения зданий, относящейся к ним инфраструктуры и людей в результате террористических нападений».[38] К серии руководящих принципов также относятся FEMA 427 («Учебник по проектированию коммерческих зданий для противодействия террористическим атакам»), FEMA 428 («Учебник по проектированию безопасных школ в случае террористических атак»), FEMA 429 («Учебник по страхованию, финансам и инструкции для управления рисками терроризма в зданиях»), FEMA 430 (архитектор) и FEMA 438 (учебный курс).

FEMA 426 не связан непосредственно с информационной безопасностью, но в состоянии предотвратить утечку, потерю или разрушение информации из-за физических атак на здания. В частности, FEMA 426 тесно связан с планом обеспечения непрерывности бизнес-процессов, который является компонентом административной безопасности. Придерживаясь FEMA 426, может быть защищен физический аспект плана обеспечения непрерывности бизнес-процессов.

Технический аспект

Для технических аспектов не существует СУИБ. Вместо них могут использоваться общепринятые международные стандарты оценки, такие как сертификация по Общим критериям (ОК).

Сертификация по Общим критериям[39]

Сертификация по ОК имеет коммерческие корни. Она была создана для решения проблемы различий в уровнях безопасности ИТ-продуктов из разных стран. Канада, Франция, Германии, Великобритания и США учредили международный стандарт для оценки ИТ-продукта.

В частности, стандарт ОК содержит требования по ИТ-безопасности продукта или системы в соответствии с отдельными категориями функциональных требований и требований обеспечения. Функциональные требования ОК определяют требуемое поведение безопасности. Требования обеспечения являются основанием для получения уверенности в том, что заявленные меры по безопасности эффективны и осуществлены надлежащим образом. Функции безопасности ОК состоят из 136 компонентов от 11 классов, сгруппированных в 57 семейств. Требования обеспечения разделены на 86 компонентов из девяти классов, составленных из 40 семейств.

Функциональные требования безопасности (ФТБ): ФТБ определяют все функции безопасности для Объекта оценки (ОО). В таблице 7 перечислены классы функций безопасности, включенных в ФТБ.

38 Там же.
39 Common Criteria, http://www.commoncriteriaportal.org.

Таблица 7. Состав классов ФТБ

Классы		Описание
FAU	Аудит безопасности	Относится к функциям, которые включают защиту данных проверки, выбор формата записи и событий, а также инструменты анализа, сигналы тревоги и анализ в режиме реального времени
FCO	Связь	Описывает требования, особенно интересов ОО, которые используются для переноса информации
FCS	Криптографическая поддержка	Определяет использование управления шифровальным ключом и шифровальных операций
FDP	Защита данных пользователя	Определяет требования, относящиеся к защите данных пользователя
FIA	Идентификация и аутентификация	Определяет требования для функций установления и подтверждения личности заявленного пользователя
FMT	Управление безопасностью	Определяет управление нескольких аспектов функций безопасности ОО (ФБОО): атрибуты безопасности, данные ФБОО и функции ФБОО
FPR	Приватность	Описывает требования, которые могли бы быть предъявлены для удовлетворения требований конфиденциальности пользователей, когда разрешается гибкость системы до тех пор, пока возможно поддерживать достаточный контроль операций системы
FPT	Защита функций безопасности объекта оценки	Содержит группы функциональных требований, относящихся к целостности и управлению механизмов, составляющих ФБОО и целостность данных ФБОО
FRU	Использование ресурсов	Содержит доступность необходимых ресурсов, таких как способность обработки и/или емкость хранения
FTA	Доступ к объекту оценки	Определяет функциональные требования для контроля создания сессии пользователя
FTP	Доверенный маршрут/ канал	Предоставляет требования для доверенных коммуникационных маршрутов между пользователями и ФБОО

Источник: Общие критерии, Общая методология для оценки безопасности информационных технологий, сентябрь 2007 г., CCMB-2007-09-004

Компоненты обеспечения безопасности (КОБ): Философия ОК требует рассматривать вместе угрозы безопасности и обязательства к политике организационной безопасности через соответствующие и надлежащие меры безопасности. Меры, которые необходимо принять, должны помочь определить уязвимости, снизить вероятность того, что ими могут воспользоваться, а также уменьшить степень ущерба в случае такой вероятности.[40] В таблице 8 перечислены классы, включенные в КОБ.

40 Common Criteria, *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements* (August 1999, Vesion 2.1), http://www.scribd.com/doc/2091714/NSA-Common-Critira-Part3.

Таблица 8. Состав классов в КОБ

Классы		Описание
APE	Оценка профиля защиты (ПЗ)	Требуется для демонстрации того, что ПЗ является работоспособным и внутренне последовательным, и, если ПЗ построен на основе одного или нескольких других ПЗ или пакетов ПЗ, то данное ПЗ является правильной реализацией примененных ПЗ и пакетов ПЗ.
ASE	Оценка задания по безопасности (ЗБ)	Требуется для демонстрации того, что ЗБ присутствует и является внутренне последовательным, и, если ЗБ основывается на одном или нескольких ПЗ или пакетов ПЗ, то данное ЗБ соответствует этим ПЗ и пакетам ПЗ.
ADV	Разработка, проектирование объекта	Обеспечивает информацией об ОО. Полученная информация используется в качестве основы для проведения анализа уязвимости и тестирования по ОО, как описано в классах ATE и AVA.
AGD	Руководство администратора и пользователя	Для безопасной подготовки и работы ОО необходимо описать все соответствующие аспекты безопасного управления ОО. Данный класс также рассматривает возможности ненамеренной неправильной конфигурации или управления ОО.
ALC	Поддержка жизненного цикла	В жизненном цикле продукта, который включает способности управления конфигурацией (УК), охват УК, поставку, безопасность разработки, исправление пороков, определение жизненного цикла, инструменты и методики, данный класс выявляет, находится ли ОО под ответственностью разработчика или пользователя.
ATE	Тестирование	Задачей данного класса является подтверждение того, что ФБОО работает согласно своему проектному описанию. Данный класс не обеспечивает глубокое тестирование.
AVA	Оценка уязвимостей	Деятельность по оценке уязвимостей охватывает анализ различных видов уязвимостей в процессе разработки и работы ОО.
ACO	Управление конфигурацией	Определяет требования доверия, которые предусмотрены для обеспечения уверенности того, что созданный ОО будет безопасно работать при условии, что основанная на безопасности функциональность будет обеспечена предварительно оцененной программой, компонентами встроенной ПО и аппаратных средств.

Источник: Общие критерии, Общая методология для оценки безопасности информационных технологий, сентябрь 2007 г., CCMB-2007-09-004

Методы оценки ОК

1. **Оценка ПЗ:** ПЗ описывает независимые от выполнения наборы требований по безопасности для категорий ОО и содержит утверждение проблемы по безопасности, которое соответствующий продукт намерен разрешить. ПЗ определяет функциональные требования и требования обеспечения ОК, а также предоставляет обоснование отобранным функциональным компонентам и компонентам обеспечения. Как правило, создается потребителем или сообществом потребителей по требованиям безопасности ИТ.

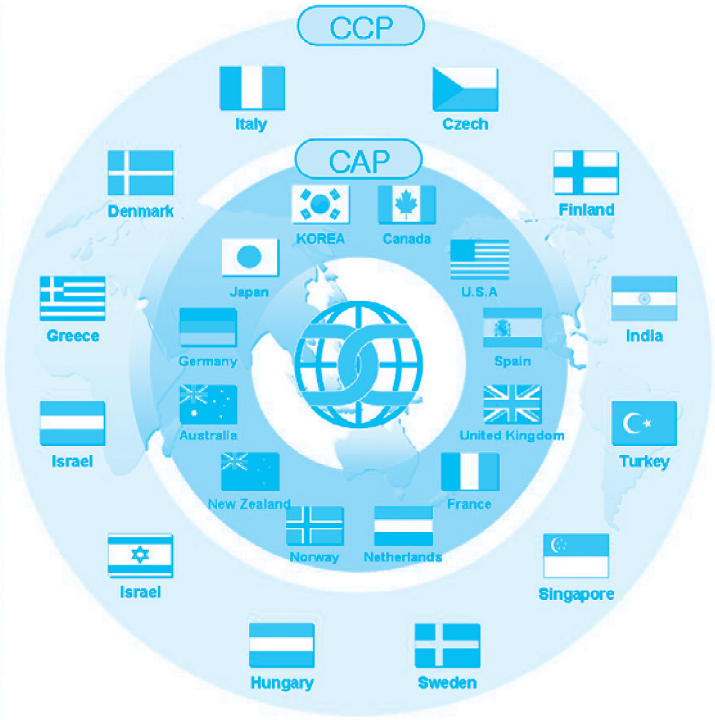
2. **Оценка ЗБ:** ЗБ является основанием для достижения соглашения между разработчиками ОО, потребителями, оценщиками и органами по оценке относительно той безопасности, которую предлагает ОО, а также ЗБ содержит охват оценки. Аудитория для формулирования ЗБ может также включать тех, кто осуществляет управление, маркетинг, покупку, установку, конфигурирование, эксплуатацию и использование ОО. ЗБ содержит информацию, имеющую некоторое отношение к эксплуатации и которая демонстрирует соответствие продукта требованиям безопасности. ЗБ может относиться к одному или нескольким ПЗ. В этом случае ЗБ должна выполнять общие требования безопасности, содержащиеся в каждом из этих ПЗ, и может определять дальнейшие потребности.

Соглашение о признании сертификатов Общих критериев

Соглашение о признании сертификатов Общих критериев (Common Criteria Recognition Arrangement, CCRA) было создано для одобрения сертификатов ОК между странами. Цель данного соглашения состоит в обеспечении выполнения следующих положений: оценки ОК осуществлены согласно соответствующим стандартам; устранение или уменьшение дублирования оценок ИТ-продуктов или профилей защиты; и повышение возможностей глобального рынка для ИТ-индустрии путем признания сертификатов среди стран-членов.

CCRA поддерживается 24 странами-членами, из которых 12 являются авторизированными участниками по сертификации (Certificate Authorizing Participants, CAP) и 12 – участниками-потребителями сертификатов (Certificate Consuming Participants, CCP). CAP – это производители сертификатов оценки. Они выступают спонсорами соответствующего сертифицирующего органа, осуществляющего деятельность в своей стране, и санкционируют выпущенные сертификаты. Страна должна быть членом CCRA в качестве CCP в течение как минимум двух лет, прежде чем сможет подать заявку на то, чтобы стать CAP. CCP – это потребители сертификатов оценки. Хотя они могут и не обладать способностью оценивать ИТ-безопасность, у них есть ярко выраженный интерес к использованию сертифицированных/утвержденных продуктов и профилей защиты. Чтобы стать членом CCRA, страна должна подать письменную заявку в Управляющий Комитет.

Рисунок 9. CAP и CCP



4.2 Примеры методологий по информационной безопасности

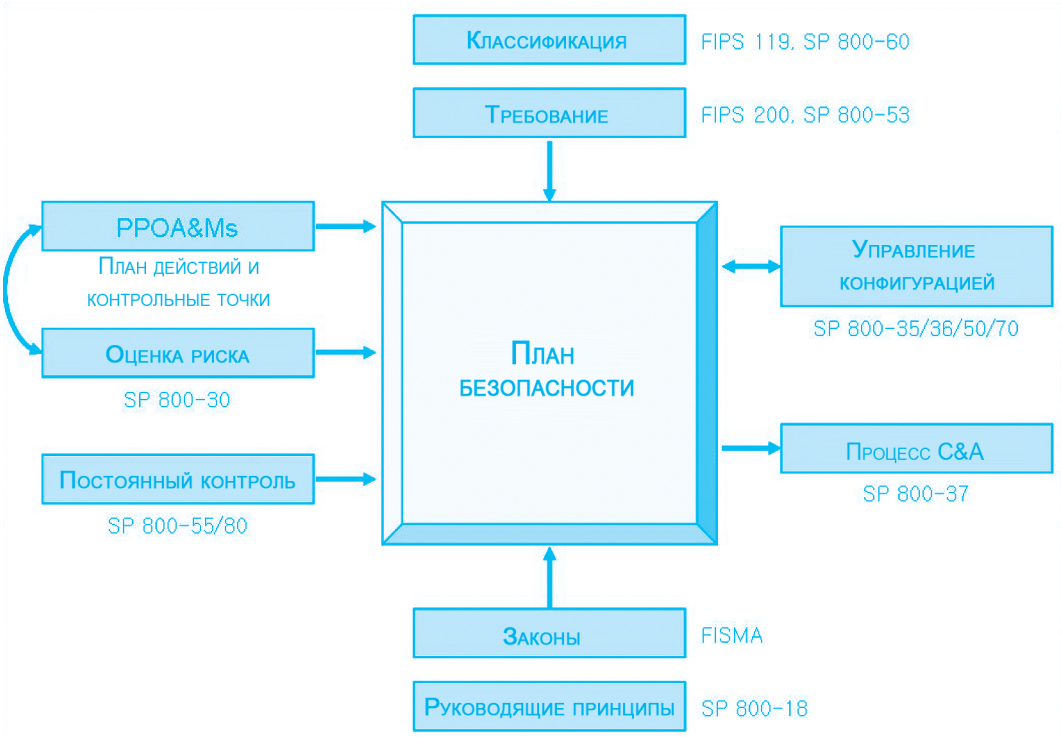
Национальный институт стандартов и технологий США

На основе FISMA Национальный институт стандартов и технологий США (НИСТ) разработал руководящие принципы и стандарты в целях укрепления безопасности информации и информационных систем, которые могут быть использованы федеральными учреждениями. Руководящие принципы и стандарты направлены на:

- Обеспечение спецификации минимальных требований безопасности путем разработки стандартов, которые могут быть использованы для классификации федеральной информации и информационных систем;
- Создание категоризации безопасности информации и информационных систем;
- Выбор и определение средств контроля безопасности для информационных систем, поддерживающих исполнительные органы власти Федерального правительства;
- Подтверждение действенности и эффективности средств контроля безопасности в случае уязвимости.

Руководящие принципы, связанные с FISMA, публикуются в качестве специальных изданий и публикаций стандартов обработки федеральной информации. Существуют две серии специальных публикаций: серия 500 по информационным технологиям и серия 800 по компьютерной безопасности. На рисунке 10 показан процесс, которому следуют правительственные организации США при создании планов безопасности на основе данного стандарта.

Рисунок 10. Ввод/вывод процесса планирования безопасности



Великобритания (BS7799)

Как было упомянуто ранее, Британский институт стандартов (BSI) анализирует деятельность организаций по обеспечению безопасности в Великобритании и выдает сертификат BS7799, который теперь был доработан до стандарта ISO27001 (BS7799 часть 2) и ISO27002 (BS7799 часть 1). На рисунке 11 показана процедура по сертификации.

Рисунок 11. Процесс сертификации BS7799

Япония (от СУИБ Ver2.0 к BS7799 часть 2: 2002)

Стандарт СУИБ Ver2.0 Японской корпорации по развитию обработки информации применяется в Японии с апреля 2002 года. Недавно он был заменен на стандарт BS7799 часть 2: 2002.

Поскольку центральное правительство поощряет процесс планирования информационной безопасности, число поданных заявок на сертификацию увеличилось. Местные органы власти предоставили организациям субсидии для прохождения сертификации СУИБ. Вместе с тем, СУИБ Ver2.0 лишь подчеркивает административный аспект и не включает в себя технический аспект информационной безопасности. Кроме того, большинство организаций заинтересовано только в том, чтобы быть сертифицированным и не обязательно в целях повышения их деятельности по обеспечению информационной безопасности.

На рисунке 12 показана система сертификации СУИБ в Японии.

Рисунок 12. Сертификация СУИБ в Японии

Республика Корея (ISO/IEC27001 и/или СУИБ KISA)

В то время как стандарт ISO/IEC 27001 распространялся организацией BSI-Корея, в стране использовалась сертификация СУИБ Корейского агентства по информационной безопасности (KISA), разработанная главным образом Министерством информатизации и коммуникации (MIC). СУИБ KISA представляет собой комбинированную систему управления, которая включает в себя план обеспечения технической/физической безопасности. Таким образом, система сертификации СУИБ KISA укрепляет техническую область информационной безопасности, которая недостаточно представлена в ISO/IEC27001. В частности, принятие «Процедуры обеспечения безопасности» в качестве требования сертификации усиливает техническую экспертизу. Рисунок 13 показывает процесс сертификации СУИБ KISA.

Рисунок 13. Сертификация СУИБ KISA

(Источник: KISA, 2005, «Процедура заявления для сертификации СУИБ», http://www.kisa.or.kr/index.jsp)

Германия (Квалификация по базовому уровню защиты ИТ)

Организация BSI Германии (Bundesamt fűr Sicherheit in der Informationstechnik) является Федеральным агентством по информационной безопасности, которое предоставляет услуги по обеспечению безопасности в области ИТ правительству, городам, организациям и частным лицам в Германии.

BSI учредил Квалификацию по базовому уровню защиты ИТ на основе международного стандарта ISO Guide 25[GUI25] и Европейского стандарта EN45001, который признается Европейским комитетом по тестированию и сертификации в области ИТ. Видами сертификации являются Сертификат по базовому уровню защиты ИТ, учрежденный самостоятельно (более высокий уровень базовой защиты ИТ) и учрежденный самостоятельно (начальный уровень базовой защиты ИТ).

Кроме того, были разработаны руководство по базовому уровню защиты (Baseline protection manual, BPM) и дополнение к руководству серии по стандарту BSI:100-X. Их содержание включает: стандарт BSI 100-1 ISMS, стандарт BSI 100-2 методологии BPM и стандарт анализа риска 100-3 BSI.[41]

Другие

В таблице 9 перечислены другие существующие сертификаты СУИБ.

Таблица 9. Сертификация СУИБ других стран

Институты сертификации		Стандарты
Канада	Предприятие по безопасности коммуникаций	Руководство MG-4 A по сертификации и аккредитации систем в области информационных технологий
Тайвань	Бюро по стандартам, метеорологии и инспекциям	CNS 17799 & CNS 17800
Сингапур	Комитет стандартов в области информационных технологий	SS493: Часть 1 (Основы стандартов безопасности в области ИТ) & SS493: Часть 2 (служба безопасности) на стадии разработки

41 Antonius Sommer, “Trends of Security Strategy in Germany as well as Europe” (presentation made at the 2006 Cyber Security Summit, Seoul, Republic of Korea, 10 April 2006), http://www.secure.trusted-site.de/download/newsletter/vortraege/KISA.pdf.

5. ОБЕСПЕЧЕНИЕ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ

Задачи данного раздела:
- **Отслеживание изменений в понятии неприкосновенности частной жизни;**
- **Описание международных тенденций в обеспечении неприкосновенности частной жизни;**
- **Обзор и примеры Оценки воздействия на неприкосновенность частной жизни (Privacy Impact Assessment).**

5.1 Понятие неприкосновенности частной жизни

Персональная информация – это любая информация, относящаяся к определению индивидуума[42] или идентификации физического лица.[43] Она включает в себя такую информацию, как имя человека, телефонный номер, адрес, адрес электронной почты, номер водительских прав, физические особенности (размеры лица, отпечатки пальцев, почерк и т.д.), номер кредитной карточки, а также семейные отношения.

Несоответствующий доступ, сбор, анализ и использование личной информации человека оказывает воздействие на поведение других лиц в отношении данного лица, и, в конечном счете, оказывает негативное влияние на его/ее социальное положение, собственность и безопасность. Таким образом, персональная информация должна быть защищена от неправомерного доступа, сбора, хранения, анализа и использования. В этом смысле персональная информация является объектом для защиты.

Когда объектом для защиты становится право на персональную информацию, а не непосредственно сама персональная информация, то это относится к понятию неприкосновенности частной жизни. Существует пять способов объяснить право на неприкосновенность частной жизни:

- Право быть свободным от нежелательного доступа (например, физический доступ, доступ через службы коротких сообщений)
- Право не допускать использование персональной информации нежелательным образом (например, продажа, разглашение, сопоставление информации)
- Право не допускать сбор персональной информации без ведома и согласия владельца, (например, с помощью системы видеонаблюдения и «cookie-файлов»)
- Право на представление персональной информации точным и корректным образом (целостность)
- Право на получение вознаграждения за стоимость собственной информации

Пассивное понятие неприкосновенности частной жизни включает в себя право возможности остаться наедине и естественное право, связанное с чувством собственного достоинства человеческой личности. Это связано с законом, запрещающим нарушение границ владения.

42 Cabinet Office, *Privacy and Data-sharing: The way forward for public services* (April 2002), http://www.epractice.eu/resource/626.

43 EurLex, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,” http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46.

Активное понятие неприкосновенности частной жизни включает в себя контроль над персональной информацией или право распоряжаться/управлять личной информацией в положительном направлении, в том числе право вносить исправления в последствия неверного представления персональной информации.

5.2 Тенденции политики обеспечения неприкосновенности частной жизни

Основные положения о защите неприкосновенности частной жизни, рекомендуемые ОЭСР

В 1980 году ОЭСР приняла «Основные положения о защите неприкосновенности частной жизни и международных обменов персональными данными», также известные как «Принципы обращения с персональными данными, рекомендуемые ОЭСР». В 2002 году был выпущен документ «Неприкосновенность частной жизни в онлайне: Руководство ОЭСР по вопросам политики и практики».[44] Основные положения применяются к персональным данным, будь то в государственном или частном секторах, которые создают угрозу для частной жизни и индивидуальных свобод из-за способа обработки информации или в силу его характера или контекста, в котором они используются. Принципы, рекомендуемые ОЭСР, перечисленные в Основных положениях, обрисовывают в общих чертах права и обязанности индивидуумов в контексте автоматизированной обработки персональных данных, а также права и обязательства тех, кто участвует в данном процессе обработки. Кроме того, основные принципы, описанные в Основных положениях, применимы как на национальном, так и на международном уровнях.

Восемь принципов Основных положений ОЭСР по защите неприкосновенности частной жизни:

1. **Принцип ограничения объема собираемых данных**

   Объем собираемых персональных данных должен иметь пределы; все эти данные должны быть получены законным и честным образом — если возможно, то с ведома или согласия субъекта данных.

2. **Принцип качества данных**

   Персональные данные должны соответствовать целям, для которых они будут использоваться, и по мере необходимости в соответствии с упомянутыми целями персональные данные должны быть достоверными, полными и регулярно обновляемыми.

3. **Принцип конкретизации целей**

   Цели, для которых собираются персональные данные, должны быть конкретизированы не позднее момента сбора указанных данных, а их последующее использование должно ограничиваться достижением упомянутых либо сходных (совместимых) целей, которые должны указываться каждый раз, когда эти цели пересматриваются.

44 OECD, “Privacy Online: OECD Guidance on Policy and Practice,” http://www.oecd.org/document/49/0,3343,en_2649_34255_19216241_1_1_1_1,00.html.

4. Принцип ограничений на использование данных

Персональные данные не должны разглашаться, предоставляться в пользование или иным образом использоваться в других целях, чем те, что перечислены в принципе конкретизации целей, за исключением случаев, когда субъект данных дает на то свое согласие или на основании закона.

5. Принцип обеспечения безопасности

Персональные данные должны быть обеспечены должными механизмами защиты от рисков, связанных с потерей, несанкционированным доступом, уничтожением, использованием, изменением или разглашением данных.

6. Принцип открытости

Процесс развития, а также практика и политика в отношении персональных данных должны осуществляться в рамках общей политики открытости. Средства должны быть легко доступны для установления факта наличия и характера персональных данных, основных целей их использования, а также личности и обычного местонахождения распорядителя данных.

7. Принцип индивидуального участия

Индивидуум должен иметь право:

а. Получать от распорядителя данных либо иным образом подтверждения того, имеются ли у распорядителя данных персональные данные, относящиеся к упомянутому индивидууму;
б. Получать относящиеся к нему персональные данные в разумные сроки; если взимается плата, то по тарифу, не являющемуся чрезмерно высоким; в рамках разумной процедуры; в удобной для понимания форме;
в. В случае отказа от удовлетворения заявки, не предоставления информации, поданной в соответствии с пунктами (а) и (б), получать разъяснения о мотивах отказа и опротестовывать такой отказ;
г. Опротестовывать относящиеся к нему данные; в случае удовлетворения протеста требовать того, чтобы таковые данные были уничтожены, исправлены или дополнены.

8. Принцип ответственности

Распорядитель данных должен нести ответственность за принятие мер, обеспечивающих соблюдение вышеперечисленных принципов.[45]

Основные положения о защите неприкосновенности частной жизни, рекомендуемые ООН

С конца 1960-ых годов мир обратил внимание на воздействие автоматизированной обработки информации на неприкасаемость частной жизни. В частности, ЮНЕСКО проявило интерес к вопросам неприкосновенности частной жизни и ее защите, так как в 1990 году Генеральной Ассамблеей были приняты «Основные положения ООН по вопросам регламентации компьютеризированной обработки персональных данных».

45 To read the entire document where these principles are listed, see the “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Основные положения ООН применяются к документам (официальным бумагам), так же как к компьютеризированным файлам данных в государственных или частных секторах. Основные положения устанавливают ряд принципов относительно минимальных гарантий, которые обеспечиваются национальным законодательством или внутренними законами международных организаций, следующим образом:

1. **Принцип законности и справедливости**

   Информация о людях не должна быть собрана или обработана нечестными или незаконными способами, и при этом не должна использоваться вопреки целям и принципам устава Организации Объединенных Наций.

2. **Принцип обеспечения точности**

   Люди, ответственные за компилирование данных или за их хранение, должны обязательно осуществлять регулярные проверки точности и уместности записанных данных и гарантировать их целостную сохранность насколько это возможно для предотвращения ошибочных упущений, их регулярное обновление или в то время, когда информация, содержащаяся в файле на хранении, используется до тех пор, пока эти данные обрабатываются.

3. **Принцип определения цели**

   Цель, которой файл с данными должен удовлетворять и использоваться с точки зрения этой цели, должна быть конкретной, законной, и, когда она установлена, должна получать определенный уровень публичности или быть представленной вниманию заинтересованного лица, чтобы впоследствии можно было гарантировать, что:

   а. Все собранные и занесенные персональные данные относятся и соответствуют указанным целям;
   б. Ни одни из упомянутых персональных данных не используются или раскрываются в целях, расходящимися с заданными, кроме как с согласия лиц, к которым относятся эти данные;
   в. Период, в течение которого хранятся персональные данные, не превышает того, которое позволяет достичь заданных целей.

4. **Принцип обеспечения доступа заинтересованного лица**

   Каждый, кто предоставляет документ, удостоверяющий личность, имеет право знать, обрабатывается ли касающаяся его/ее информация, и получить это в доступной форме, без излишней задержки или затрат, а также выполнить соответствующие исправления или уничтожение в случае незаконных, ненужных или неточных записей и быть при возможности информированным об адресатах.

5. **Принцип обеспечения недискриминации**

   С учетом исключительных случаев, предусмотренных в принципе 6, данные, которые могут привести к незаконной или произвольной дискриминации, в том числе информация о расовой принадлежности или этнического происхождения, цвета кожи, пола, политических взглядов, религиозных, философских и других убеждений, а также членство в объединении или профсоюзе, не должны собираться.

6. Компетенция для определения исключений

Отступления от принципов 1–4 могут быть разрешены только в том случае, если они необходимы для защиты национальной безопасности, общественного порядка, здоровья или нравственности, а также, среди прочего, прав и свобод других, особенно преследуемых лиц (принцип гуманности), при условии, что такие отступления четко определены в законе или соответствующем нормативном документе, принятом в соответствии с внутренней правовой системой, которая явно устанавливает их пределы и устанавливает соответствующие гарантии.

Исключения из принципа 5, касающиеся запрета дискриминации, в дополнение к тому, чтобы быть подчиненным тем же самым гарантиям, как предписано для исключений из принципов 1 и 4, могут быть разрешены только в пределах, предписанных Международным биллем о правах человека и другими соответствующими документами в области защиты прав человека и предотвращения дискриминации.

7. Принцип обеспечения безопасности

Должны быть приняты соответствующие меры для защиты файлов с данными как от естественных опасностей, так и случайных потерь или разрушений, а также угроз, связанных с человеческой деятельностью, таких как: несанкционированный доступ, мошенническое злоупотребление данными или заражение компьютерными вирусами.

8. Надзор и санкции

В соответствии с внутренней законодательной системой каждая страна должна назначить орган власти, который должен нести ответственность за надзор соблюдения принципов, изложенных выше. Данный орган власти должен предложить гарантии беспристрастности, независимости в отношении лиц или учреждений, ответственных за обработку и установление информации, а также техническую компетентность. В случае нарушения положений национального законодательства, осуществляющего вышеупомянутые принципы, должны быть предусмотрены уголовные или иные наказания с соответствующими индивидуальными мерами.

9. Трансграничные потоки данных

Когда законодательство двух или более стран, вовлеченных в процесс международного обмена данных, предлагает сопоставимые гарантии для защиты неприкосновенности частной жизни, информация должна быть в состоянии распространяться также свободно, как и внутри каждой из территорий. Если нет никаких взаимных гарантий, ограничения на такое распространение не могут налагаться незаконно и только до тех пор, пока требуется защита неприкосновенности частной жизни.

10. Область применения

Существующие принципы должны быть применимы, прежде всего, ко всем государственным и частным компьютерным файлам данных с помощью возможного расширения и с учетом соответствующих поправок к рукописным файлам. Специальные положения, также по выбору, могли бы расширить действия всех или части принципов к файлам на юридических лиц, особенно если они содержат информацию об индивидуумах.[46]

46 The principles are quoted from the Office of the High Commissioner for Human Rights, “Guidelines for the Regulation of Computerized Personal Data Files,” http://www.unhchr.ch/html/menu3/b/71.htm.

Директива ЕС о защите данных

В дополнение к регулированию базовых основ безопасности вокруг персональной информации повсеместно, где она хранится, передается или обрабатывается, 24 октября 1995 года Совет министров ЕС принял Европейскую директиву о защите физических лиц при обработке персональных данных и свободном перемещении этих данных (Директива ЕС) для создания нормативной базы по обеспечению безопасного и свободного перемещения персональных данных через государственные границы стран-членов ЕС.

Директива ЕС о защите данных была создана с целью объединить и согласовать с муниципальными нормативными актами, связанными с защитой неприкосновенности частной жизни. Статья 1 Директивы ЕС объявляет о том, что «Страны-члены должны защищать основные права и свободы физических лиц, и, в частности, их право на неприкосновенность частной жизни в связи с обработкой персональных данных».

Директива ЕС запрещает передачу персональной информации странам, в которых отсутствует соответствующий уровень защиты, что приводит к антагонизму в отношениях между ЕС и администрацией США.[47]

Для обеспечения исполнения Директивы ЕС каждая страна, являющаяся членом ЕС, пересмотрела свои существующие законы или учредила новые законы о защите неприкосновенности частной жизни.

К другим примерам законов ЕС о защите неприкосновенности частной жизни относятся Статья 8 Европейской Конвенции по правам человека, Директива 95/46/ЕС (Директива о защите данных), Директива 2002/58/ЕС (Директива об электронной неприкосновенности частной жизни) и Статья 5 Директивы 2006/24/ЕС (Директива по хранению данных).[48]

Защита неприкосновенности частной жизни в Республике Корея

Республика Корея имеет наибольшее число абонентов широкополосной сети в мире. В первой половине 2005 года к широкополосным сетям были подсоединены 75 процентов домохозяйств и 25 процентов населения.[49] Сегодня беспроводные коммуникации и широкополосные сети Республики Корея признаны одними из лучших в мире. Таким образом, частота утечки персональной информации в стране значительно возросла, что требует как политических, так и технологических решений.

Тем не менее, правительство Кореи не продвинулось в этом направлении достаточно быстро. Закон о защите неприкосновенности частной жизни по-прежнему находится на рассмотрении в Национальном Собрании. Также не существует отдельного закона по защите персональной информации.

С другой стороны, правительство Кореи приняло «Среднесрочную и долгосрочную «дорожную карту» по обеспечению информационной безопасности для реализации программы u-SafeKorea» и с 2005 года реализует четыре важнейших приоритетных проекта: (1) обеспечение безопасности современной инфраструктуры; (2) установление доверия при оказании новых ИТ-услуг; (3) усиление функций информационной защиты для новых двигателей роста; (4) создание базы информационной безопасности в новой

47 Domingo R. Tan, Comment, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union, 21 LOY. L.A. INT'L & COMP. L.J. 661, 666 (1999).
48 Justice and Home Affairs, "Data Protection," European Commission, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.
49 Internet World Stats, "Korea," Miniwatts Marketing Group, http://www.internetworldstats.com/asia/kr.htm.

киберсреде. Четвертый приоритет включает подпроект под названием «Укрепление системы защиты неприкосновенности частной жизни».

Крометого,существуютнесколькозаконов,которыесвязанысзащитойнеприкосновенности частной жизни, например: «Закон о защите персональной информации в обществе» или «Закон о телекоммуникационных сетях и защите информации».

Закон о защите персональной информации в обществе: Данный закон содержит положения, касающиеся обработки и управления персональной информации, обработанной в компьютерах государственных учреждений для защиты неприкосновенности частной жизни, а также положения, связанные с надлежащим исполнением государственных дел и защитой прав и интересов людей.

Акт о поощрении использования информационных и коммуникационных сетей и защите информации: Цель этого закона состоит в улучшении системы защиты конфиденциальности частного сектора, так как происходит расширение информационно-коммуникационных сетей и конвергенции процессов сбора и распространения персональной информации. Акт регулирует процесс защиты неприкосновенности частной жизни на основе таких этапов жизненного цикла персональной информации, как сбор, использование, управление и удаление. Также закон содержит положения, связанные с правами пользователей личной информации, а также учреждение и работу комитета по вмешательству в частную жизнь.

Акт о защите секретности при коммуникации: Акт ограничивает целевой диапазон действия неприкосновенности частной жизни и свободы общения для защиты неприкосновенности частной жизни в процессе коммуникации и обеспечения свободы общения. Закон запрещает вторжение в секретную беседу путем производства записи или перехвата сообщений, и он защищает неприкосновенность частной жизни при коммуникациях.

Закон о защите информации о местонахождении: Акт направлен на регулирование сбора и использования информации, имеющей отношение к местонахождению; для защиты против утечек, неправильного употребления/злоупотребления такой информации, а также содействия использованию информации в безопасной среде. Закон признает потенциал современных информационных технологий по определению местонахождения того или иного лица (например, через мобильные телефоны), а также факт того, что утечка информации о местонахождении может вызвать серьезные нарушения неприкосновенности частной жизни. Таким образом, закон содержит правило: никогда не раскрывать информацию о местонахождении, за исключением случаев, когда этого требует закон.

Защита неприкосновенности частной жизни в США

США возложили деятельность по защите неприкосновенности частной жизни на рынок, поскольку слишком много правительственных ограничений препятствует деятельности электронной коммерции. В результате появились такие компании по обеспечению режима неприкосновенности частной жизни, как Trust-e или «Better Business Bureau Online» (Бюро по совершенствованию онлайн-бизнеса), и законы о защите неприкосновенности частной жизни не являются интегрированными. Закон об охране частной жизни от 1974 года предусматривает защиту конфиденциальности информации в государственном секторе, в то время как различные законы регулируют конфиденциальность в частном

секторе. Не существует организации, занимающейся всеми вопросами защиты конфиденциальности в частном секторе. В государственном секторе согласно закону об охране частной жизни роль в создании политики по обеспечению неприкосновенности частной жизни федерального правительства играет Административно-бюджетное управление (АБУ) США. В частном секторе выполнять законы, защищающие неприкосновенность частной жизни детей в Интернете, кредитную информацию клиента и добросовестную конкуренцию уполномочена Федеральная комиссия по торговле.

Законы США, связанные с защитой неприкосновенности частной жизни:

- Закон об охране частной жизни от 1974 г.
- Закон о защите потребительского кредита от 1984 г.
- Закон о неприкосновенности в сфере электрических коммуникаций от 1986 г.
- Акт Грэма-Лича-Блилей от 1999 г. (Gramm-Leach-Bliley Act, 1999)
- Закон о преемственности страхования и отчетности в области здравоохранения от 1996 г.
- Акт Сарбаниса-Оксли от 2002 г. (Sarbanes-Oxley Act, 2002)
- Закон о защите неприкосновенности частной жизни детей в Интернете от 1998 г.

Меры по защите неприкосновенности частной жизни в Японии

В 1982 году Япония установила меры по защите неприкосновенности частной жизни на основе восьми основных принципов ОЭСР. В 1988 году был принят и вступил в силу закон о защите неприкосновенности частной жизни в государственном секторе. В частном секторе Министерством внешней торговли и промышленности в 1997 году было издано Руководство по защите неприкосновенности частной жизни. Для улучшения соответствия национальных законов о защите неприкосновенности частной жизни с международными руководящими принципами Главное управление по развитию общества передовых ИКТ (Advanced Information and Telecommunications Society Promotion Headquarters) инициировало проект по разработке закона о защите неприкосновенности частной жизни.

Кроме того, в качестве независимого агентства было создано Управление по защите данных, которое обеспечивает надлежащее соблюдение защиты неприкосновенности частной жизни и оказывает помощь лицам в случае вторжения в частную жизнь. Управление по защите данных уполномочено проводить работы по улучшению прозрачности обработки информации, обеспечению прав и выгод субъектов данных, а также гарантирование выполнения своих обязанностей как агентства по обработке информации, так и пользователей информации. Управление, как ожидается, также будет играть важную роль при защите национальных интересов, особенно в случаях передачи информации через государственные границы.

Законы Японии, связанные с защитой неприкосновенности частной жизни, включают следующее:

- Закон о защите личных данных, обработанных на компьютере административными органами, 1988 г.
- Регламенты для местных органов власти (приняты в 1999 году для 1529 местных органов власти)
- Закон о защите персональной информации, 2003 г.
- Закон о защите персональной информации при осуществлении административными органами своей деятельности, 2003 г.

- Закон о защите персональной информации при осуществлении своей деятельности независимыми административными учреждениями от 2003 г.
- Закон об аудиторской комиссии, 2003 г.
- Основные положения о защите неприкосновенности частной жизни при использовании меток радиочастотной идентификации (RFID), 2004 г.

Вопросы для размышлений

1. Какая политика осуществляется, и какие существуют законы о защите конфиденциальности информации в вашей стране?

2. Какие вопросы или соображения влияют на принятие и/или осуществление такой политики и законов?

3. Какие принципы (см. Основные положения ОЭСР и ООН), по вашему мнению, лежат в основе политики и законов по защите неприкосновенности частной жизни в вашей стране?

5.3 Оценка воздействия на неприкосновенность частной жизни

Что собой представляет оценка воздействия на неприкосновенность частной жизни?

Оценка воздействия на неприкосновенность частной жизни (Privacy Impact Assessment, PIA) является непрерывным процессом изучения, анализа и оценки воздействия введения новых информационных систем или модификации существующих информационных систем на неприкосновенность частной жизни клиентов или граждан. PIA основан на «принципе раннего предупреждения», то есть «профилактика лучше лечения». Это не просто оценка системы, а также рассмотрение серьезного воздействия введения или изменения новых систем на неприкосновенность частной жизни. Таким образом, она отличается от аудита обеспечения защиты неприкосновенности частной жизни, которая обеспечивает соблюдение внутренней политики и внешних требований для неприкосновенности частной жизни.

Поскольку PIA проводится для анализа фактора нарушения неприкосновенности частной жизни при создании новой системы, данный процесс должен быть выполнен на ранней стадии разработки, когда еще возможны уточнения спецификации разработки. Однако, когда во время эксплуатации существующей службы происходит серьезный риск вторжения при сборе, использовании и управлении персональной информацией, желательно осуществить PIA, а затем усовершенствовать соответственно систему.

Процесс PIA[50]

Процесс PIA обычно состоит из трех этапов (Таблица 10).

50 This section is drawn from Information and *Privacy Office, Privacy Impact Assessment: A User's Guide* (Ontario: Management Board Secretariat, 2001), http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Таблица 10. Процесс PIA

Концептуальный анализ	Анализ потока данных	Последующий анализ
Подготовить словесное описание исследуемой области и деловое обоснование предложенной инициативы. Предварительно определить потенциальные проблемы и риски для неприкосновенности частной жизни и ключевые заинтересованные стороны. Предоставить детальное описание значимых аспектов предложения, включая политический анализ основных вопросов. Вести учет основных потоков персональной информации. Составить обзор проблем окружающей среды для изучения того, как другие юрисдикции осуществляли подобные инициативы. Определить вопросы и проблемы заинтересованных сторон. Оценить общественную реакцию.	Проанализировать потоки данных посредством диаграмм бизнес-процессов и определить свойственные элементы персональных данных или кластеров данных. Оценить соответствие предложений с принципом свободы распространения информации (freedom of information, FOI) и законодательством по обеспечению неприкосновенности частной жизни, а также уставами соответствующих программ. Оценить более широкое соответствие предложения с общими принципами неприкосновенности частной жизни. Проанализировать риски, существующие при реализации инициативы, на основе анализа неприкосновенности частной жизни и определить возможные решения. Просмотреть варианты проектов и выявить нерешенные вопросы/ проблемы обеспечения неприкосновенности частной жизни, которые не были рассмотрены. Подготовить ответы на неразрешенные вопросы обеспечения неприкосновенности частной жизни.	Просмотреть и проанализировать физические аппаратные и системные разработки предлагаемой инициативы в целях обеспечения соблюдения требований обеспечения неприкосновенности частной жизни. Предоставить окончательный обзор предлагаемой инициативы. Провести анализ обеспечения неприкосновенности частной жизни и рисков при внесении любых новых изменений в предложенную инициативу, имеющую отношение к дизайну аппаратных средств и программного продукта, для обеспечения соблюдения FOI и законодательства о неприкосновенности частной жизни, уставов соответствующих программ, а также общих принципов неприкосновенности частной жизни. Подготовить план коммуникаций.

Источник: Служба информации и обеспечения неприкосновенности частной жизни, Оценка воздействия на неприкосновенность частной жизни: Руководство для пользователей(Ontario: Management Board Secretariat, 2001), 5, http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Условия выполнения оценки PIA

PIA осуществляется при:

1. Создании новой информационной системы, которая будет хранить и иметь дело с большим количеством информации персонального характера;
2. Использовании новой технологии, когда неприкосновенность частной жизни может быть нарушена;
3. Модифицировании существующей информационной системы, которая хранит и имеет дело с персональной информацией;
4. Сборе, использовании, хранении и/или уничтожении персональной информации, в ходе чего существует риск нарушения неприкосновенности частной жизни.

Но нет необходимости осуществлять PIA на всех информационных системах. PIA не должна выполняться при небольших изменениях существующей программы и системы.

Примеры PIA

В таблице 11 перечислены системы PIA в трех странах.

Таблица 11. Примеры национальных PIA

	США	Канада	Австралия/Новая Зеландия
Нормативно-правовая база	Раздел 208 Закона об электронном правительстве от 2002 г. АБУ сформулировало требования к PIA в документе OMB-M-03-22	Политика и основное положение о PIA приняты в мае 2002 г. Обязательное выполнение PIA на основе общего закона о неприкосновенности частной жизни	Добровольное выполнение PIA (без юридического основания) Справочник PIA для поддержки PIA (Новая Зеландия, 2004 г.), Основное положение о PIA (Австралия, 2004 г.)
Субъект	Все исполнительные филиалы управлений и агентств, а также подрядчики, которые используют ИТ или работают с веб-сайтами с целью взаимодействия с населением; соответствующие межведомственные инициативы агентств, включая те, которые содействуют электронному правительству	Все программы и услуги, предоставляемые государственными агентствами	Нет обязанностей или ограничений

	США	Канада	Австралия/Новая Зеландия
Исполнитель	Агентства, осуществляющие проекты электронного правительства и имеющие дело с персональной информацией	Правительственные органы, разрабатывающие или осуществляющие программы и услуги	Соответствующие учреждения или внешние консалтинговые агентства по запросу
Публикация	Публичная доступность PIA через веб-сайт агентства, публикация в Федеральном реестре или др. средствах, может быть изменена или отклонена по причине безопасности или для защиты секретной, деликатной или частной информации, содержащейся в оценке Агентства должны предоставить Директору АБУ копию PIA каждой системы, для которой было запрошено финансирование	Публичная доступность краткого содержания PIA Предварительное предоставление копии окончательного PIA и отчета Уполномоченному по безопасности в целях получения надлежащего совета или рекомендаций в отношении стратегии соответствующей защиты	Результат PIA, как правило, не доступен для широкой публики (не обязаны сообщать и публиковать)

Проверьте себя

1. Чем персональная информация отличается от других видов информации?
2. Почему персональная информация должна быть защищена?
3. Какое значение имеют принципы ОЭСР и ООН при защите неприкосновенности частной жизни?
4. Почему проводится оценка воздействия на неприкосновенность частной жизни?

6.0 СОЗДАНИЕ И ФУНКЦИОНИРОВАНИЕ CSIRT

Задачи данного раздела:
- **Объяснить, как создать и обеспечить управление национальной службой реагирования на инциденты компьютерной безопасности (Computer Security Incident Response Team, CSIRT);**
- **Рассмотреть модели CSIRT разных стран.**

К киберпреступности и различным угрозам информационной безопасности нужно отнестись серьезно из-за их огромного воздействия на экономику. Японская ассоциация по сетевой безопасности, например, оценила в 2006 году экономические потери от утечки частной информации приблизительно в 446 млн. долл. США – или 347 долл. США на человека. Компания Ferris Research оценила убытки от спама в США приблизительно в 8,9 млрд. долл. США в 2002 году, 20 млрд. долл. США в 2004 году и 50 млрд. долл. США в 2005 году.

Создание CSIRT является эффективным средством смягчения и минимизации ущерба от атак на информационные системы и нарушений в области информационной безопасности.

6.1 Разработка и эксплуатация CSIRT

CSIRT – это специально созданная организация, которая ответственна за получение, рассмотрение и реагирование на сообщения о компьютерных инцидентах и их действиях. Основная цель CSIRT состоит в оказании услуг по обработке компьютерных инцидентов для минимизации ущерба и эффективного восстановления после инцидента, связанного с компьютерной безопасностью.[51]

В 1988 году впервые появился «червь» по имени Моррис, который быстро распространился по всему миру. После этого Агентство по перспективным оборонным научно-исследовательским разработкам США (Defence Advanced Research Projects Agency, DARPA) основало Институт по разработке программного обеспечения (Software Engineering Institute, SEI), а затем учредило организацию CERT/CC в университете Карнеги-Меллона в соответствии с контрактом правительства США. После этого каждая страна в Европе создала аналогичные организации. Поскольку ни один CSIRT не был в состоянии решить широкий круг инцидентов уязвимости, в 1990 году был создан Форум служб безопасности и реагирования на инциденты (Forum of Incident Response and Security Teams, FIRST). Через FIRST многие агентства по информационной безопасности и различные CSIRT получили возможность обменяться мнениями и поделиться информацией.

Выбор правильной модели CSIRT[52]

Существует пять основных организационных моделей для CSIRT. Должна быть принята наиболее подходящая для организации модель при рассмотрении различных условий, таких как: окружающая среда, финансовое положение и человеческие ресурсы.

51 CERT, “CSIRT FAQ,” Carnegie Mellon University, http://www.cert.org/csirts/csirt_faq.html.

52 This section is drawn from Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

1. Модель службы безопасности (с использованием существующего ИТ-персонала)
Модель службы безопасности не является типичной моделью CSIRT. По сути, она является противоположностью общепринятой CSIRT. В этой модели нет централизованной организации, которая несет ответственность за обработку инцидентов компьютерной безопасности. Вместо этого задачи по обработке инцидентов решаются системными и сетевыми администраторами или другими специалистами по обслуживанию системы обеспечения безопасности.

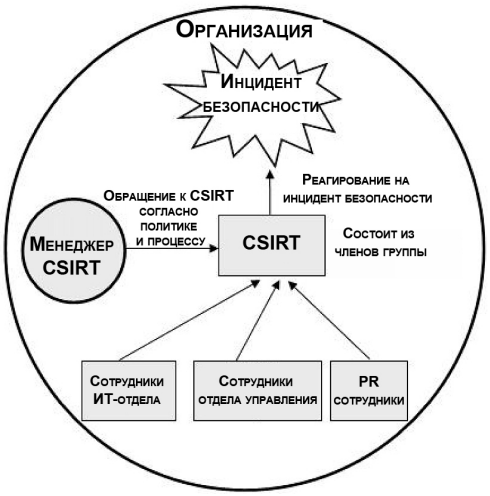
Рисунок 14. Модель службы безопасности

2. Модель внутренней распределенной CSIRT
Данную модель также называют «распределенная CSIRT». Персонал данной модели состоит из администратора CSIRT, ответственного за отчетность и общее управление, а также сотрудников из других подразделений предприятия/агентства. CSIRT в данной модели является официально признанной организацией, несущей ответственность за управление реагированием на инциденты. Поскольку служба построена в пределах компании или агентства, ее считают «внутренней».

Модель внутренней распределенной CSIRT отличается от модели службы безопасности следующим образом:

- Существование более формализованной политики, процедур и процессов по реагированию на инциденты;
- Определенный способ связи со всем предприятием по вопросам угроз безопасности и стратегий реагирования;
- Наличие менеджера CSIRT и членов команды, которые специально назначены для решения задач по реагированию на инцидент.

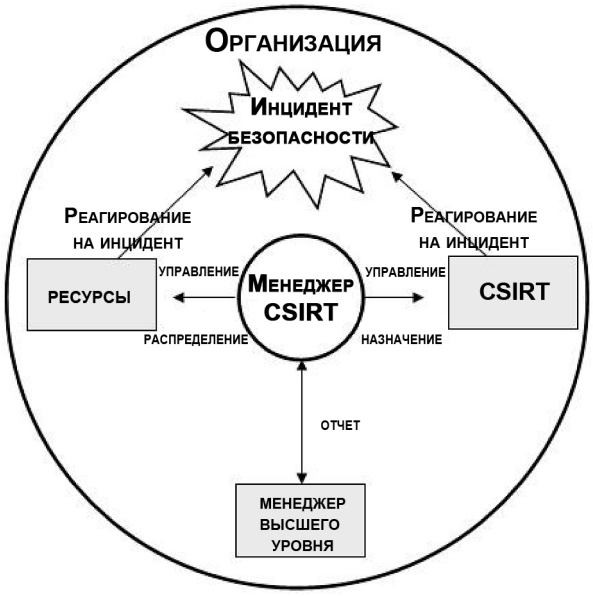
Рисунок 15. Модель внутренней распределенной CSIRT



3. Модель внутренней централизованной CSIRT

В модели внутренней централизованной CSIRT команда, расположенная в центре, контролирует и поддерживает жизнедеятельность организации. CSIRT несет общую ответственность за отчетность, анализ и реагирование на все инциденты. Таким образом, участники команды не могут выполнять другую работу и проводят все свое время, работая на службу и реагируя на все инциденты. Кроме того, менеджер CSIRT отчитывается вышестоящему руководству: главному информационному управляющему (Chief Information Officer), главному специалисту по безопасности (Chief Security Officer) или главному специалисту по рискам (Chief Risk Officer).

Рисунок 16. Модель внутренней централизованной CSIRT

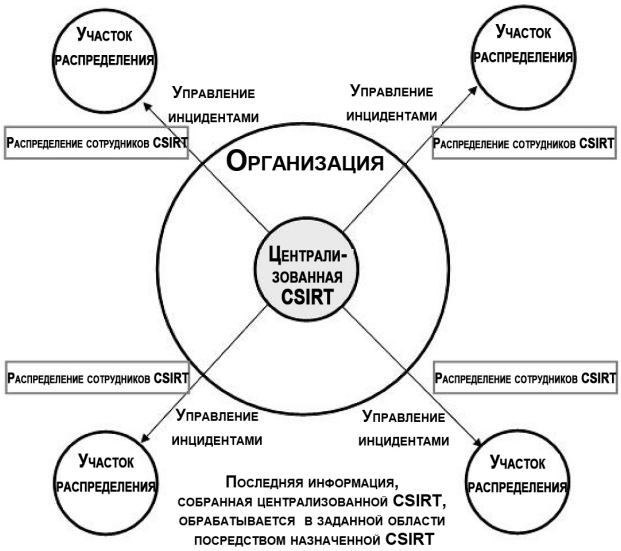


4. Модель комбинированной распределенной и централизованной CSIRT

Модель также известна как «комбинированная CSIRT». В тех случаях, когда централизованная CSIRT не может контролировать и поддерживать всю организацию, некоторые участники команды распределены по участкам/ветвям/подразделениям организации для обеспечения в пределах своих областей ответственности тот же уровень услуг, как это предусмотрено в централизованной CSIRT.

Централизованная группа обеспечивает анализ данных высокого уровня, методы восстановления и стратегии уменьшения опасностей. Она также предоставляет поддержку сотрудникам распределенной службы в реагировании на инциденты, уязвимости и повреждения. Сотрудники распределенной группы осуществляют на каждом участке стратегию и обеспечивают экспертизу в своих областях.

Рисунок 17. Комбинированная CSIRT



5. Модель координационной CSIRT

Координационная CSIRT усиливает функцию распределенных служб в комбинированной CSIRT. В модели координационной CSIRT сотрудники службы в комбинированной CSIRT сгруппированы в независимые CSIRT по таким характеристикам, как: подключение к сети, географические границы и т.п. Они находятся под управлением централизованной CSIRT.

Модель координационной CSIRT является подходящей для национальной системы CSIRT. Данная модель может быть применена для внутренней деятельности организации, а также для поддержки и тесного сотрудничества с внешними агентствами.

Деятельность по координации и содействию включает обмен информацией, обеспечение стратегии смягчения последствий, реагирование на инциденты, методы восстановления, исследование/анализ тенденций и характера деятельности инцидентов, создание баз данных уязвимости, информационные центры для инструментов по безопасности, услуги по предоставлению консультаций и оповещений.

Рисунок 18. Координационная CSIRT

Учреждение CSIRT: этапы по созданию национальных CSIRT[53]

Существует пять этапов в создании CSIRT. Цель, видение или роли CSIRT должны служить ориентиром в последовательности этапов.

Этап 1 – Обучение заинтересованных сторон развитию национальной службы

Этап 1 – это информирующая стадия, где заинтересованные стороны достигают понимания того, что требуется для создания CSIRT. С помощью различных методов обучения они изучают:

а. Стимулирующие бизнес-процессы и мотивы, стоящие за необходимостью создания национальной CSIRT;
б. Требования для развития потенциала, необходимого национальной CSIRT, для реагирования на инциденты;
в. Выявление людей, которые будут вовлечены в обсуждения для построения национальной службы;
г. Ключевые ресурсы и критическая инфраструктура, которые существуют внутри страны;
д. Типы каналов коммуникаций, которые должны быть определены для связи с клиентами CSIRT;
е. Специальные законы, нормативы и другие политические методы, которые будут влиять на развитие национальной CSIRT;
ж. Стратегии финансирования, которые могут быть использованы для развития, планирования, осуществления и управления способностью по реагированию;
з. Технологическая и сетевая информационная инфраструктура, которая будет необходима для поддержки работы национальной службы;
и. Основные планы реагирования и взаимозависимости ввиду их применения в многочисленных секторах;
к. Потенциальный список основных услуг, которые национальная CSIRT может оказать своим клиентам;
л. Передовой опыт и практические руководства

53 This section is drawn from Georgia Killcrece, *Steps for Creating National CSIRTs* (Pittsburgh: Carnegie Mellon University, 2004), http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

Этап 2 – Планирование CSIRT: построение на основе знаний и информации, полученных на этапе 1

Этап 2 предполагает планирование CSIRT, основанной на знаниях и информации, полученной на этапе 1. Вопросы, рассмотренные на этапе 1, пересматриваются и обсуждаются далее, и затем определяются и применяются точные детали для выполнения плана. План создается с учетом следующих видов деятельности:

а. Идентификация требований и потребностей национальной CSIRT —
   - Законы и нормативы, которые будут влиять на работу национальной службы
   - Критические ресурсы, которые должны быть определены и защищены
   - Текущие инциденты и тенденции, о которых известно или должны быть известно
   - Существующие квалификации по реагированию на инциденты и экспертиза в области компьютерной безопасности

б. Определение концепции национальной CSIRT
в. Формулирование миссии национальной службы
г. Определение клиентуры (или клиентов), которую она будет обслуживать
д. Идентификация коммуникационных интерфейсов между клиентурой и национальной службой
е. Определение со стороны государства того, кто будет утверждать, вести и спонсировать
ж. Определение категорий навыков и знаний персонала, которые необходимы для управления службой
з. Определение типов функций и обязанностей национальной CSIRT
и. Спецификация процессов управления инцидентами CSIRT, также как определение взаимоотношений с аналогичными процессами в любой из внешних организаций-клиентов
к. Разработка стандартизированного набора критериев и единой терминологии для категоризации и определения действий и случаев инцидентов
л. Определение методов взаимодействия национальной CSIRT с клиентурой и другими глобальными CSIRT или внешними партнерами
м. Определение любых процессов, которые необходимо интегрировать в существующие планы по восстановлению после аварий, по реагированию на инциденты, планы по обеспечению бизнес-непрерывности, планы по управлению в кризисной или других чрезвычайных ситуациях
н. Разработка календаря проекта
о. Создание плана национальной CSIRT на основе результатов деятельности планирования, концепции и соответствующей базовой структуры

Этап 3 – Реализация CSIRT

Для реализации CSIRT на этапе 3 команда по реализации проекта использует информацию и планы, разработанные на этапах 1 и 2. Процесс реализации состоит из следующих действий:

а. Получение финансовых средств из источников, определенных на этапе планирования
б. Широкомасштабное объявление о создании национальной CSIRT и о том, где можно получить дополнительную информацию (о прогрессе в развитии, требованиях по отчетности и т.д.)
в. Согласование механизмов координации и коммуникации с заинтересованными сторонами и другими соответствующими контактными лицами

г. Внедрение безопасных информационных систем и сетевой инфраструктуры для работы национальной CSIRT (например, защищенные серверы, приложения, телекоммуникационное оборудование и другие ресурсы поддержки инфраструктуры)
д. Разработка регламентов работы и процессов для персонала CSIRT, в том числе согласованный стандарт на стадии планирования и руководство по отчетности
е. Разработка внутренней политики и процедур для доступа и работы оборудования CSIRT и персонального оборудования, а также приемлемой политики использования
ж. Осуществление процессов для взаимодействий национальной CSIRT с ее клиентами
з. Выявление и наем (или переназначение) персонала, предоставления соответствующей профессиональной подготовки и образования для персонала CSIRT, а также определение других потенциальных привлекательных возможностей для обучения и образования клиентов

Этап 4 – Эксплуатация CSIRT

На этапе эксплуатации определены основные услуги, которые должна предоставлять национальная CSIRT, и дана оценка эксплуатационной эффективности использования возможностей реагирования на инциденты. На основе данных результатов рассмотрены и усовершенствованы операционные моменты. Деятельность на данном этапе представляет следующее:

а. Активное предоставление различных услуг, оказываемых национальной CSIRT
б. Разработка и осуществление механизма оценки эффективности работы национальной CSIRT
в. Совершенствование работы национальной CSIRT по результатам оценки
г. Расширение миссии, услуг и численности персонала, соответствующих и устойчивых для увеличения обслуживания клиентуры
д. Продолжение развития и укрепления политики и процедур CSIRT

Этап 5 – Сотрудничество

Национальная CSIRT может развивать доверительные отношения с ключевыми заинтересованными сторонами на основе эффективной работы (Этап 4). Но национальная CSIRT также нуждается в обмене важной информацией и опытом по обработке инцидентов на основе долгосрочных обменов в сотрудничестве с учреждениями, внутренними и международными CSIRT. Деятельность на данном этапе включает в себя:

а. Участие в деятельности по обмену данными и информацией, а также поддержке разработки стандартов для обмена данными и информацией между партнерами, другими CSIRT, клиентами и другими экспертами по вопросам компьютерной безопасности
б. Участие в глобальных акциях «наблюдения и предупреждения» для поддержки сообщества CSIRT
в. Повышение качества деятельности CSIRT путем организации профессиональной подготовки, семинаров и конференций, на которых обсуждаются тенденции нападений и стратегии реагирования
г. Сотрудничество с другими членами сообщества для разработки документов передового опыта и руководящих принципов
д. Рассмотрение и пересмотр процессов по управлению инцидентами, как часть постоянного процесса совершенствования

Услуги CSIRT[54]

Услуги, которые оказывают CSIRT, могут быть классифицированы в реагирующие услуги, упреждающие услуги и услуги по управлению качественным обслуживанием.

Реагирующие услуги являются основными услугами CSIRT. Они включают в себя:

1. Оповещения и предупреждения – Данные услуги включают в себя предоставление информации и методов реагирования для решения таких проблем, как уязвимость безопасности, оповещение о вторжении, компьютерный вирус или обман.

2. Обработка инцидентов – Данный сервис включает в себя получение, сортировку и реагирование на запросы и сообщения, анализ и определение приоритетности инцидентов и событий. Конкретные ответные мероприятия включают в себя следующее:

    - Анализ инцидента – экспертиза всей доступной информации и подтверждающих доказательств или артефактов, связанных с инцидентом или событием. Цель такого анализа состоит в том, чтобы определить масштабы этого инцидента, степень ущерба, нанесенного инцидентом, природу инцидента и доступных стратегий или методов реагирования.

    - Сбор вещественных доказательств – сбор, хранение, документирование и анализ доказательств подвергшейся риску компьютерной системы для определения изменений в системе и оказания помощи в реконструкции событий, приведших к риску.

    - Отслеживание и розыск – включает отслеживание или розыск того, как злоумышленник получил доступ в поврежденные системы и связанные с ними сети. Данная деятельность включает в себя отслеживание происхождения непрошенного гостя или выявление систем, к которым злоумышленник имел доступ.

3. Реагирование на инциденты на месте – CSIRT обеспечивает непосредственную помощь на месте для того, чтобы помочь клиентам оправиться от инцидента.

4. Поддержка реагирования на инцидент – CSIRT помогает и руководит жертвой(-ами) нападения при восстановлении от инцидента с помощью телефона, электронной почты, факса или документации.

5. Координация реагирования на инцидент – Координируются усилия по реагированию среди сторон, вовлеченных в инцидент. Они, как правило, включают в себя жертву нападения, другие стороны, вовлеченные при атаке, а также любые стороны, нуждающиеся в помощи при анализе атаки. Это может также включать стороны, которые оказывают ИТ-поддержку жертве, такие как ISP и другие CSIRT.

6. Действия при обнаружении уязвимости – Это предполагает получение информации и сообщений об уязвимости аппаратных средств и программного обеспечения, анализ последствий уязвимости и разработку стратегий реагирования для выявления и устранения уязвимости.

54 This section is drawn from Carnegie Mellon University, *CSIRT Services* (2002), http://www.cert.org/archive/pdf/CSIRT-services-list.pdf.

- Анализ уязвимости – Относится к техническому анализу и экспертизе уязвимости аппаратных средств или программного обеспечения. Данный анализ может включать пересмотр исходного кода с использованием отладчика для определения происхождения уязвимости или попытку воспроизвести проблему на тестовой системе.

- Реагирование на уязвимость – Подразумевает определение надлежащих мер для смягчения или устранения уязвимостей. Данная служба может включать в себя осуществление реагирования путем установления исправлений, закрепления или обхода. Она также включает уведомление других о стратегиях смягчения последствий, рекомендации и предупреждения.

- Координация реагирования на уязвимости – CSIRT уведомляет различные отделы предприятия или клиентов об уязвимости и делится информацией о том, как устранить или смягчить опасность. CSIRT также классифицирует успешные стратегии реагирования на уязвимости. Мероприятия включают в себя анализ уязвимости или сообщения об уязвимости, а также обобщение технического анализа, проделанные различными сторонами. Данная служба может также включать ведение государственного или частного архива или базы знаний с информацией об уязвимости и соответствующих ответных мер.

7. Обслуживание артефакта – Данный сервис состоит из анализа, реагирования, координации и обработки артефактов, связанных с компьютерными вирусами, программами «Троянский конь», «червями», используемыми скриптами и инструментарием.

    - Анализ артефакта – CSIRT выполняет техническую экспертизу и анализ любого артефакта, найденного в системе.

    - Реагирование на артефакт – Включает определение надлежащих мер для обнаружения и удаления артефактов из системы.

    - Координация реагирования на артефакт – Включает обмен и обобщение результатов анализа и стратегий реагирования, имеющих отношение к артефакту, с другими исследователями, CSIRT, поставщиками и другими экспертами по безопасности.

Упреждающие услуги предоставляются для улучшения инфраструктуры и процессов безопасности клиентов до того, как будет обнаружен какой-либо инцидент или событие, имевшее место. Они включают в себя следующее:

1. Уведомления – Они включают сигналы тревоги, предупреждения уязвимости, консультации о безопасности и т.п. Такие уведомления сообщают клиентам о новых разработках от среднесрочного до долгосрочного влияния, как, например, недавно обнаруженные уязвимости или инструменты злоумышленника. Уведомления позволяют клиентам защитить свои системы и сети от только что обнаруженных проблем прежде, чем они могут быть использованы.

2. Отслеживание технологий – Это предусматривает мониторинг и наблюдение за новыми техническими разработками, деятельностями злоумышленников и связанными тенденциями, чтобы помочь определить будущие угрозы. Результатом данной услуги может быть какой-либо руководящий принцип или рекомендации, ориентированные на средне- и долгосрочные вопросы безопасности.

3. Оценки или аудит безопасности – Данная услуга предоставляет подробный обзор и анализ инфраструктуры безопасности организации, основанные на требованиях, установленных в организации или другими отраслевыми стандартами, которые применяются.

4. Настройка и обслуживание средств безопасности, приложений, инфраструктуры и услуг – Данный сервис предоставляет соответствующие указания о том, как безопасно настроить и обслуживать средства, приложения и общую вычислительную инфраструктуру.

5. Разработка средств по обеспечению безопасности – Эта услуга включает в себя разработку новых средств с учетом запросов клиентов, программного обеспечения, плагинов и заплаток, которые разрабатываются и распространяются в целях обеспечения безопасности.

6. Услуги по обнаружению вторжений – CSIRT, которые предоставляют данные услуги, пересматривают существующие журналы систем по обнаружению вторжений (Intrusion Detection Systems, IDS), анализируют их и приступают к реагированию на события, которые возникают в пределах их действия.

7. Распространение информации, связанной с безопасностью – Эти услуги предоставляют клиентам всеобъемлющий и простой сборник полезной информации, которая помогает в повышении безопасности.

Услуги по управлению качеством безопасности призваны предоставлять знания, полученные в результате искусственного реагирования на инциденты, уязвимости и нападения. Такие услуги включают:

1. Анализ рисков – Он предполагает усовершенствование возможностей CSIRT по оценке реальных угроз, обеспечению реалистичных качественных и количественных оценок рисков для информационных ресурсов, а также оценке защиты и стратегий реагирования.

2. Планирование непрерывности бизнес-процессов и восстановления после аварий – непрерывность бизнес-процессов и восстановление после аварий, вызванных атаками на систему компьютерной безопасности, обеспечиваются путем надлежащего планирования.

3. Консультация по безопасности – CSIRT могут также предоставить практические советы и рекомендации для осуществления бизнес-операций.

4. Повышение информированности – CSIRT в состоянии повысить уровень осведомленности по вопросам безопасности путем выявления и предоставления информации и рекомендации по поводу методов и политики безопасности, необходимых клиентам.

5. Образование/Обучение – Данная услуга включает предоставление образования и подготовку кадров по таким темам, как руководящие принципы по составлению отчетов об инцидентах, соответствующие методы реагирования, средства реагирования на инциденты, методы предотвращения инцидентов, а также иную информацию, необходимую для защиты, обнаружения, сообщения и реагирования на инциденты компьютерной безопасности. Учебные методы включают в себя конференции, семинары, курсы и обучающие программы.

6. Оценка или сертификация продукции – CSIRT могут проводить оценки продукта с помощью средств, приложений или других услуг для обеспечения безопасности продукции и их соответствия приемлемым CSIRT или организационным практическим уровням безопасности.

Таблица 12 показывает уровень каждой услуги CSIRT — т.е. является ли она основной, дополнительной или исключительной — в каждой модели CSIRT.

Таблица 12. Услуги CSIRT

Категория услуг	Услуги		Служба безопасности	Распределенная	Централизованная	Комбинированная	Координирующая
Реагирующая	Предупреждения		Дополнительная	Основная	Основная	Основная	Основная
	Обработка инцидента	Анализ инцидента	Основная	Основная	Основная	Основная	Основная
		Реагирование на инцидент на месте	Основная	Дополнительная	Дополнительная	Дополнительная	Исключительная
		Поддержка реагирования на инцидент	Исключительная	Основная	Основная	Основная	Основная
		Координирование реагирования на инцидент	Основная	Основная	Основная	Основная	Основная
	Обработка артефактов	Анализ уязвимости	Дополнительная	Дополнительная	Дополнительная	Дополнительная	Дополнительная
		Реагирование на уязвимости	Основная	Дополнительная	Исключительная	Дополнительная	Дополнительная
		Координирование реагирования на уязвимости	Дополнительная	Основная	Основная	Основная	Основная
		Анализ артефакта	Дополнительная	Дополнительная	Дополнительная	Дополнительная	Дополнительная
		Реагирование на артефакт	Основная	Дополнительная	Дополнительная	Дополнительная	Дополнительная
		Координирование реагирования на артефакт	Дополнительная	Дополнительная	Основная	Основная	Основная
Упреждающая	Уведомления		Исключительная	Основная	Основная	Основная	Основная
	Отслеживание технологий		Исключительная	Дополнительная	Основная	Основная	Основная
	Оценка или проверка безопасности		Исключительная	Дополнительная	Дополнительная	Дополнительная	Дополнительная
	Конфигурация и эксплуатация инструментов безопасности, приложений, инфраструктур и услуг		Основная	Дополнительная	Дополнительная	Дополнительная	Исключительная
	Разработка инструментов безопасности		Дополнительная	Дополнительная	Дополнительная	Дополнительная	Дополнительная
	Услуги по обнаружению вторжений		Основная	Дополнительная	Дополнительная	Дополнительная	Исключительная
	Распространение информации, относящейся к безопасности		Исключительная	Дополнительная	Основная	Основная	Основная
Управление качеством безопасности	Анализ риска		Исключительная	Дополнительная	Дополнительная	Дополнительная	Исключительная
	Планирование непрерывности бизнес-процессов и восстановления после аварий		Исключительная	Дополнительная	Дополнительная	Дополнительная	Исключительная
	Консультации по безопасности		Исключительная	Дополнительная	Дополнительная	Дополнительная	Исключительная
	Повышение информированности		Исключительная	Дополнительная	Дополнительная	Дополнительная	Основная
	Образование/ обучение		Исключительная	Дополнительная	Дополнительная	Дополнительная	Основная
	Оценка или сертификация продукта		Исключительная	Дополнительная	Дополнительная	Дополнительная	Исключительная

Источник: Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

6.2 Международные CSIRT

В настоящее время существует ряд специализированных международных CSIRT, созданных для реагирования на инциденты в области компьютерной безопасности во всем мире. В то время как национальные CSIRT могут ответить на атаки и выполнить свои другие функции, международные атаки требуют внимания международной CSIRT.

Форум служб безопасности и реагирования на инциденты[55]

Форум служб безопасности и реагирования на инциденты (Forum of Incident Response Security Teams, FIRST) состоит из CERT, государственных агентств и компаний по обеспечению безопасности из 41 страны. В его состав входят 191 организаций, в том числе CERT/CC и US-CERT. FIRST является учреждением для обмена информацией и сотрудничества между службами реагирования на инциденты. Его цель состоит в активизации деятельности по реагированию на инциденты и защите, и мотивации сотрудничества среди участников путем предоставления технологий, знаний и средств для реагирования на инциденты. К деятельности FIRST относится:

- Разработка и обмен передовым опытом, методиками, инструментами, технической информацией и методологиями реагирования на инциденты и защиты;
- Стимулирование развития политики, услуг и продуктов безопасности хорошего качества;
- Поддержка и развитие соответствующих руководящих принципов по компьютерной безопасности;
- Оказание помощи правительствам, предприятиям и образовательным учреждениям по созданию и расширению службы реагирования на инциденты;
- Содействие обмену технологиями, опытом и знаниями между участниками в целях обеспечения более безопасной электронной среды.

Азиатско-Тихоокеанская CERT[56]

Азиатско-Тихоокеанская Служба реагирования на непредвиденные ситуации в компьютерах (Asia-Pacific Computer Emergency Response Team, APCERT) было создана в феврале 2003 года в качестве сетевого сообщества экспертов по безопасности для усиления потенциала реагирования на инциденты и повышения осведомленности по вопросам безопасности в Азиатско-Тихоокеанском регионе. Первая конференция Азиатско-Тихоокеанской CSIRT была проведена в Японии в 2002 году. APCERT была создана год спустя на конференции в Тайпее, в которой приняли участие 14 Азиатско-Тихоокеанских CSIRT. По состоянию на август 2007 года у APCERT было 14 постоянных членов и шесть ассоциированных членов.

Участники APCERT признали, что сегодня инциденты в области компьютерной безопасности являются слишком многочисленными, сложными и трудными для управления в рамках одной организации или страны, и что более эффективное реагирование может быть развернуто на основе сотрудничества с другими членами APCERT. Как и в FIRST, наиболее важным понятием в APCERT являются доверительные отношения между участниками для обмена информацией и взаимодействия друг с другом. Таким образом, мероприятия APCERT направлены на:

- Расширение Азиатско-Тихоокеанского регионального и международного сотрудничества;

55 FIRST, “About FIRST,” FIRST.org, Inc., http://www.first.org/about/.
56 APCERT, “Background,” http://www.apcert.org/about/background/index.html.

- Совместную выработку мер для борьбы с инцидентами в области безопасности в крупномасштабных или региональных сетях;
- Улучшение обмена информацией и технологиями в области безопасности, в том числе информацией о компьютерных вирусах, использованных скриптах и т.п.;
- Повышение эффективности совместных исследований по общим проблемам;
- Содействие другим CERT в регионе по эффективному реагированию на инциденты в области компьютерной безопасности;
- Предоставление консультаций и решений юридических вопросов, связанных с региональной информационной безопасностью и реагированием на инциденты.

Европейская правительственная CERT[57]

Европейская правительственная CERT (European Government CERT, EGC) является неофициальным комитетом, который ассоциируется с CSIRT в европейских странах. Ее членами являются Финляндия, Франция, Германия, Венгрия, Нидерланды, Норвегия, Швеция, Швейцария и Великобритания. Роль и функции этого комитета заключаются в следующем:

- Совместная разработка мер для борьбы с инцидентами в области безопасности в крупномасштабных или региональных сетях;
- Содействие обмену информацией и технологиями в связи с инцидентами в области безопасности, угрозами от использования вредоносного кода и уязвимостями;
- Определение областей знаний и опыта, которые могут быть совместно использованы внутри группы;
- Определение областей для совместных научных исследований и разработок по темам, которые представляют интерес для участников;
- Содействие формированию правительственных CSIRT в европейских странах.

Европейское агентство по сетевой и информационной безопасности[58]

Целью Европейского агентства по сетевой и информационной безопасности (European Network and Information Security Agency, ENISA) является повышение сетевой и информационной безопасности (СИБ) в Европейском союзе путем создания культуры в области СИБ. Оно было учреждено в январе 2004 года Советом министров и Европейским парламентом для реагирования на «высокотехнологичные» преступления. Агентство выполняет следующие задачи:

- Оказание поддержки в целях обеспечения СИБ среди членов ENISA или ЕС;
- Содействие устойчивому обмену информацией между заинтересованными сторонами;
- Улучшение координации функций, имеющих отношение к СИБ.

ENISA, как ожидается, должно внести свой вклад в международные усилия по смягчению воздействия вирусов, взлома и созданию системы мониторинга угроз в онлайне.

6.3 Национальные CSIRTs

Ряд стран организовали свои национальные CSIRT. В таблице 13 перечислены страны и их соответствующие CSIRT, а также вебсайты каждой службы.

57 EGC, http://www.egc-group.org.
58 ENISA, “About ENISA,” http://www.enisa.europa.eu/pages/About_ENISA.htm.

Таблица 13. Перечень национальных CSIRT

Страна	Официальное название	Домашняя страница
Аргентина	Служба реагирования на компьютерные инциденты государственной администрации Аргентины	http://www.arcert.gov.ar
Австралия	Служба реагирования на компьютерные инциденты Австралии	http://www.aucert.org.au
Бразилия	Служба реагирования на компьютерные инциденты Бразилии	http://www.cert.br
Бруней Даруссалам	Служба реагирования на компьютерные инциденты Брунея	http://www.brucert.org.bu
Канада	Готовность к чрезвычайным ситуациям по обеспечению общественной безопасности Канады	http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp
Чили	Служба реагирования на компьютерные инциденты Чили	http://www.clcert.cl
Китай	Национальная техническая служба реагирования на инциденты в компьютерных сетях – Координационный центр Китая	http://www.cert.org.cn
Дания	Служба реагирования на компьютерные инциденты Дании	http://www.cert.dk
Сальвадор	Служба реагирования на компьютерные инциденты	
Финляндия	Агентство по управлению коммуникациями Финляндии	http://www.cert.fi
Франция	CERT-Администрация	http://www.certa.ssi.gouv.fr
Германия	CERT-Bund	http://www.bsi.bund.de/certbund
Гонконг	Координационный центр реагирования на компьютерные инциденты Гонконга	http://www.hkcert.org
Венгрия	CERT- Венгрия	http://www.cert-hungary.hu
Индия	CERT-Индия	http://www.cert-in.org.in
Индонезия	Служба реагирования на компьютерные инциденты Индонезии	http://www.cert.or.id
Япония	Координационный центр CERT Японии	http://www.jpcert.or.jp
Литва	LITNET CERT	http://cert.litnet.lt
Малайзия	Служба реагирования на компьютерные инциденты Малайзии	http://www.mycert.org.my
Мексика	Мексиканский национальный автономный университет	http://www.cert.org.mx
Нидерланды	GOVCERT.NL	http://www.govcert.nl
Новая Зеландия	Центр защиты критической инфраструктуры	http://www.ccip.govt.nz
Норвегия	Норвежское управление национальной безопасности	http://www.cert.no
Филиппины	Служба реагирования на компьютерные инциденты Филиппин	http://www.phcert.org
Польша	Служба реагирования на компьютерные инциденты Польши	http://www.cert.pl

Страна	Официальное название	Домашняя страница
Катар	Служба реагирования на компьютерные инциденты Катара	http://www.qcert.org
Саудовская Аравия	Служба реагирования на компьютерные инциденты - Саудовская Аравия	http://www.cert.gov.sa
Сингапур	Служба реагирования на компьютерные инциденты Сингапура	http://www.singcert.org.sg
Словения	Служба реагирования на компьютерные инциденты Словении	http://www.arnes.si/english/si-cert
Республика Корея	Координационный центр CERT Кореи	http://www.krcert.or.kr
Испания	IRIS-CERT	http://www.rediris.es/cert
Швеция	Шведский центр по инцидентам в области ИТ	http://www.sitic.se
Таиланд	Служба реагирования на компьютерные инциденты Таиланда	http://www.thaicert.nectec.or.th
Тунис	Служба реагирования на компьютерные инциденты – Координационный центр Туниса	http://www.ansi.tn/en/about_cert-tcc.htm
Турция	TP-CERT	http://www.uekae.tubitak.gov.tr
Великобритания	GovCertUK	http://www.govcertuk.gov.uk
США	Служба реагирования на компьютерные инциденты США	http://www.us-cert.gov
Вьетнам	Служба реагирования на компьютерные инциденты Вьетнама	http://www.vncert.gov.vn

Источник: CERT, «Национальные службы реагирования на компьютерные инциденты», Carnegie Mellon University, http://www.cert.org/csirts/national/contact.html.

Практическое упражнение

Существует ли в вашей стране национальная CSIRT?

1. Если да, опишите ее в зависимости от адаптированной модели и как она работает. Оцените, насколько эффективно она выполняет свои функции.

2. Если нет, определите, какая модель CSIRT была бы подходящей для вашей страны, и опишите, что требуется для создания национальной CSIRT в вашей стране.

Проверьте себя

1. Каковы основные функции CSIRT?

2. Насколько отличаются международные CSIRT от национальных CSIRT?

3. Какие существуют требования для создания CSIRT?

7. ЖИЗНЕННЫЙ ЦИКЛ ПОЛИТИКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

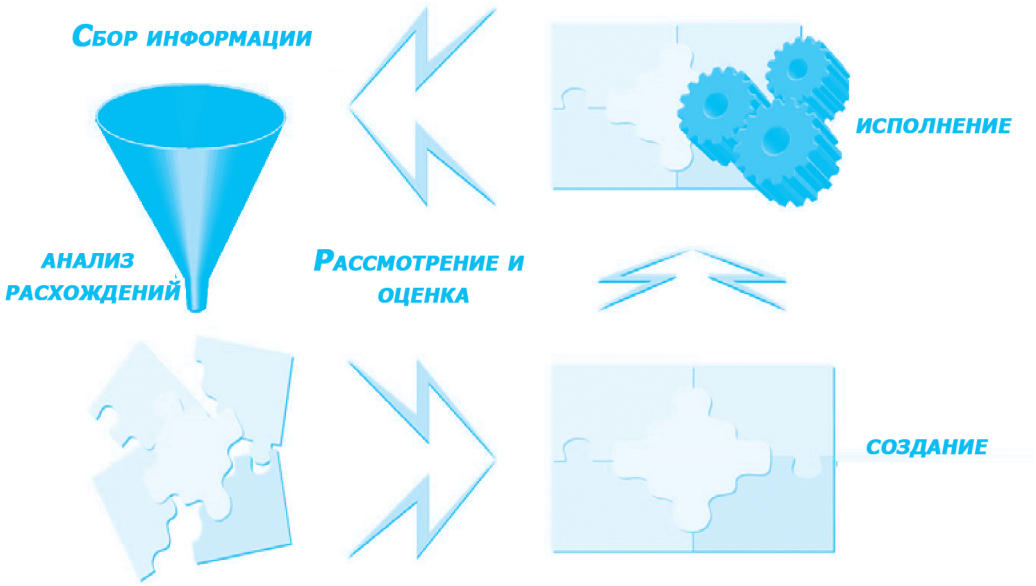
Задачи данного раздела:
- **Дать краткий обзор процесса разработки политики по информационной безопасности;**
- **Обсудить вопросы, которые необходимо учитывать при разработке политики в области информационной безопасности.**

Разработчики политики должны принять во внимание целый ряд факторов, среди которых обоснование стратегии, имеющиеся ресурсы, политика руководства, бюджетные и законодательные потребности, а также ожидаемые результаты политики. В данном разделе эти факторы рассматриваются в контексте различных этапов разработки политики в области информационной безопасности.

Следует отметить, что у разных стран будут несколько иные политические соображения и контексты. Процесс разработки политики, описанный в данном разделе, является обобщенным и основанным на предположении о том, что не существует национальной политики в области информационной безопасности.

Как и с другими политическими направлениями, жизненный цикл политики по информационной безопасности можно разделить на четыре этапа: (1) сбор информации и анализ расхождений; (2) создание политики; (3) осуществление политики; (4) контроль и обратная связь (Рисунок 19). Кроме того, национальная политика в области информационной безопасности должна включать в себя стратегию по информационной безопасности, нормативно-правовые отношения, организацию информационной безопасности, технологию информационной безопасности, а также взаимосвязи между ними.

Рисунок 19. Жизненный цикл политики по информационной безопасности



7.1 Сбор информации и анализ расхождений

Первым этапом в разработке политики по информационной безопасности является сбор информации и анализ расхождений.

При сборе информации полезно рассмотреть примеры в области информационной безопасности и политики из других стран, так и в самой стране.

При анализе расхождений важно понять существующую инфраструктуру, относящуюся к информационной безопасности, как, например, существующие законы и системы, а также области или упущения, которые должны быть восполнены. Это важный шаг, поскольку он определяет направление или приоритеты политики в области информационной безопасности.

Сбор информации

Примеры сбора информации из-за рубежа: При рассмотрении подходящих примеров других стран разработчики политики должны принимать во внимание схожесть по следующим вопросам:

- Уровень национальной информационной безопасности
- Направление создания политики
- Сетевая и системная инфраструктура

Учитывая эти сходства, должны быть собраны следующие материалы:

- Информация о создании и деятельности организаций, занятых в области информационной безопасности (см. разделы 3 и 6 настоящего модуля),
- Политика, законы и постановления в области информационной безопасности (см. раздел 3),
- Методология в области информационной безопасности, используемая в международном масштабе, и примеры других стран (см. раздел 4),
- Тенденции угроз и меры противодействия или средства управления в соответствии с типами нападений (см. разделы 2 и 6),
- Меры противодействия для защиты неприкосновенности частной жизни (см. раздел 5)

Сбор местных материалов: Хотя большинство разработчиков политики не являются экспертами в области информационной безопасности, они выполняют мероприятия, связанные или имеющие отношение к информационной безопасности. В частности, они создают законы, правила и политики в областях, связанных с информационной безопасностью. Однако, так как законы, правила и политики, как правило, концентрируют внимание на конкретных областях, корреляция между ними не может быть сразу же очевидной для разработчиков политики. Таким образом, необходимо собирать, анализировать и оценивать все законы, правила и политики, связанные или имеющие отношение к информационной безопасности.

Анализ расхождений

В книге Сунн-Цзы «Искусство побеждать» сказано: «Знай своего врага». Это означает, что вы должны знать хорошо как свои пределы, так и пределы возможностей своего

врага. В случае разработки политики в области информационной безопасности это будет означать знание того, что именно должно быть защищено с помощью политики по информационной безопасности, а также уязвимостей и угроз информационной безопасности.

Анализ расхождений можно разделить на два этапа:

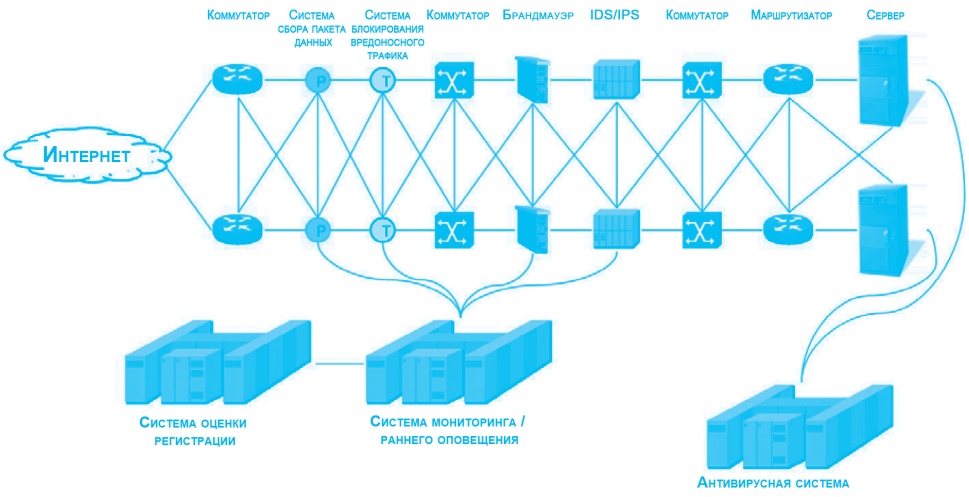
1. Понимание возможностей и потенциала страны – например, организация и человеческие ресурсы, а также информационная и коммуникационная инфраструктура – в общем обеспечении информационной безопасности;
2. Определение внешних угроз информационной безопасности.

Разработчики политики должны быть **знакомы с организацией информационной безопасности и человеческими ресурсами** — то есть с государственными и частными учреждениями в областях, связанных с информационной безопасностью. Они должны знать организации, вовлеченные в работы, связанные с информационной безопасностью, и понимать их сферу деятельности, функции и обязанности. Это важно для того, чтобы не дублировать уже существующие структуры по обеспечению информационной безопасности.

Кроме того, на этой стадии должны быть определены и задействованы эксперты в области информационной безопасности. Такие эксперты, как правило, имеют опыт работы в законодательстве, политике, технологиях, образовании и смежных областях.

Информационно-коммуникационная инфраструктура относится к структуре в области ИТ, которая осуществляет сбор, обработку, хранение, поиск, передачу и получение электронной системы контроля и информацию. Короче говоря, это информационные системы и сети. **Понимание текущего статуса информационно-коммуникационной инфраструктуры** является особенно важным с экономической точки зрения. Поскольку необходимы крупные инвестиции для подключения по всей стране, это делает большинство существующих информационно-коммуникационных инфраструктур выгодными. Рисунок 20 показывает пример информационно-коммуникационной инфраструктуры для информационной безопасности. Она не включает в себя все элементы, которые могут потребоваться, и приводится здесь только в иллюстративных целях. Обратите внимание на взаимосвязи между различными компонентами сети.

Рисунок 20. Пример сетевой и системной структуры



Разработчикам политики необходимо понимать, каким образом создаются общие сети и системы для информационной безопасности.

Вторым шагом в анализе расхождения является **определение внешних угроз информационной безопасности.** Как уже упоминалось в разделе 2, угрозы важной информации не только увеличиваются, но также становятся более изощренными. Разработчики политики должны понимать данные угрозы для того, чтобы можно было решить, какие меры противодействия необходимо предпринять. В частности разработчики политики должны понимать:

- Степень проникновения угроз информационной безопасности
- Наиболее распространенные и текущие виды атак
- Типы угроз и их ожидаемая степень интенсивности в будущем

После анализа государственных организаций, человеческих ресурсов и информационно-коммуникационной инфраструктуры, а также осознания компонентов угрозы в области информационной безопасности, важное значение имеет определение уязвимых компонентов. Это устанавливает степень, до которой страна может устоять перед внешними компонентами угроз. Это определение можно сделать, изучая следующее:

- Текущее положение дел в CERT и ее способность реагировать
- Текущий статус экспертов по информационной безопасности
- Уровень устройства и интенсивность системы информационной безопасности
- Правовая защита информационных активов от посягательств
- Физическая среда для защиты информационных активов

Цель анализа расхождения состоит в том, чтобы иметь возможность определить практические меры противодействия, которые необходимо предпринять. Следует подчеркнуть, что это самый важный шаг при разработке политики в области информационной безопасности.

7.2 Разработка политики в области информационной безопасности

Разработка национальной политики по обеспечению информационной безопасности включает в себя: (1) Определение направления политики; (2) создание организации по информационной безопасности и определение ее функций и обязанностей; (3) построение рамочной структуры политики в области информационной безопасности; (4) учреждение и/или пересмотр законов для согласования их с политикой; и (5) распределение бюджета для реализации информационной политики.

1. Установление курса политики и настойчивое продвижение

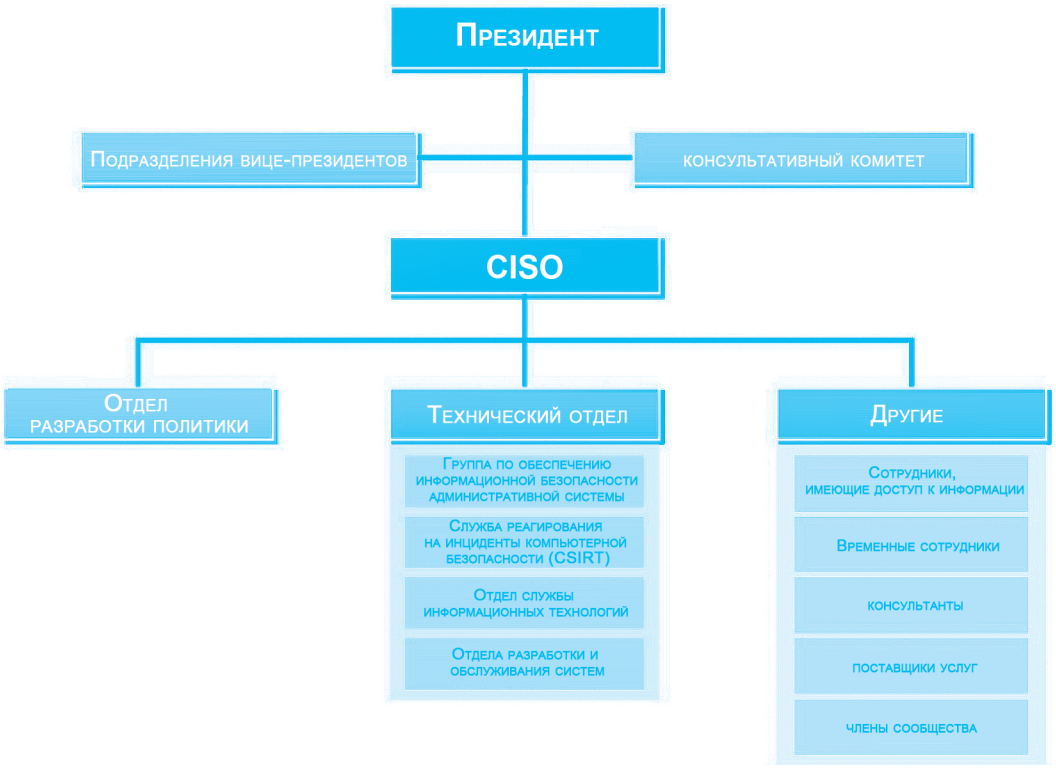
В большинстве случаев создание политики в области информационной безопасности должно инициироваться правительством, а не частным сектором. В частности, правительство должно установить политику, играть ведущую роль в деле ввода необходимой инфраструктуры на местах и оказывать долгосрочную поддержку. Частный сектор присоединяется к проекту со временем, главным образом, чтобы принять участие в исследованиях, разработке и строительстве системы.

Планирование участия частных организаций включает в себя мероприятия по повышению осведомленности наряду с созданием и укреплением информационно-коммуникационной инфраструктуры. Если правительство ставит своей целью поощрение частного сектора принять стратегию по обеспечению информационной безопасности, то правительство должно играть больше вспомогательную, а не контролирующую роль. Это включает в себя распространение руководящих принципов по информационной безопасности.

2. Создание организации по информационной безопасности и определение ее функций и обязанностей[59]

Как только устанавливается направление реализации политики по обеспечению информационной безопасности, создается организация по ее реализации. Рисунок 21 показывает структуру обобщенной государственной организации по информационной безопасности.

Рисунок 21. Пример государственной организации по информационной безопасности



Государственные организации по информационной безопасности слегка отличаются друг от друга в зависимости от особенностей и культуры каждой страны. Тем не менее, основной принцип заключается в том, чтобы роли и обязанности были четко разграничены.

59 This section is drawn from Sinclair Community College, “Information Security Organization - Roles and Responsibilities,” http://www.sinclair.edu/about/information/usepolicy/pub/infscply/Information_Security_Organization_-_Roles_and_Responsibilities.htm.

Административная организация

На **подразделении вице-президентов** лежит основная ответственность за сбор, хранение информации и/или определение ее в качестве используемой или «принадлежащей» соответствующим подразделениям. Они могут назначать должностное лицо по информационной безопасности (Information Security Officer, ISO) и других лиц для помощи ISO в осуществлении политики информационной безопасности. Эти назначенные сотрудники должны обеспечивать то, что информационные ресурсы в пределах их контролируемого пространства имеют владельцев; проводятся оценки степени риска; а также осуществляются процессы смягчения последствий рисков.

Руководители (директора, председатели, менеджеры и т.д.) управляют работниками, имеющими доступ к информации и информационным системам, и определяют, осуществляют и используют средства управления информационной безопасностью, применимые в соответствующих областях. Они должны обеспечить, чтобы все сотрудники понимали свои персональные обязанности относительно информационной безопасности, и чтобы служащие имели доступ, необходимый для выполнения своей работы. Руководители должны периодически проверять уровни доступа всех пользователей на предмет соответствия и предпринимать соответствующие меры для устранения несоответствий или недостатков.

Главный управляющий по информационной безопасности (Chief Information Security Officer, CISO) отвечает за координацию и контроль политики в области информационной безопасности. Работая в тесном сотрудничестве с различными подразделениями, CISO может рекомендовать руководителям конкретных подразделений назначить других представителей по контролю и координации определенных элементов этой политики. CISO также помогает владельцам информации передовым опытом по обеспечению информационной безопасности:

- Создание и распространение исполняемых правил в отношении доступа и приемлемого использования информационных ресурсов;
- Проведение/координация оценки и анализа степени риска информационной безопасности;
- Создание обоснованных руководящих положений и мер, направленных на защиту данных и систем;
- Оказание помощи в деле мониторинга и управления уязвимостей систем безопасности;
- Проведение/координация аудита в области информационной безопасности;
- Оказание помощи в проведении расследований/решений проблем и/или предполагаемых нарушений государственной политики в области информационной безопасности.

Техническая организация

Группа по обеспечению информационной безопасности административной системы разрабатывает и осуществляет меры по обеспечению того, что административное применение средства управления безопасностью позволяет заинтересованным сторонам соответствующий доступ к информации, и в то же время выполнение национальных правовых и этических обязательств по защите частной, засекреченной и важной информации. Группа разрабатывает процессы и стандарты для обеспечения оптимальной доступности, целостности и конфиденциальности информации административной системы, включая процессы для пользователей по запросу начального доступа и изменений доступа; документации для разрешения пользовательского доступа, а также для прав и обязанностей пользователя/руководителя; и урегулирования конфликтов и

проблем, связанных с безопасностью.

Группа включает в себя Отдел специалистов по информационной безопасности и CISO. Также группа получает консультации из Департамента специалистов по информационной безопасности и от системных администраторов государственных систем.

CSIRT предоставляет информацию и оказывает содействие заинтересованным сторонам в осуществлении превентивных мер для уменьшения рисков инцидентов компьютерной безопасности, а также в расследовании, реагировании и сведения к минимуму ущерба от таких инцидентов, когда они происходят. CSIRT также определяет и рекомендует последующие мероприятия. Двухуровневый CSIRT состоит из оперативной команды, ответственной за начальную идентификацию, реагирование, сортировку и определение требований при эскалации, а также команды управления, ответственной за государственное реагирование на крупные и серьезные инциденты. Составной частью оперативной CSIRT являются CISO и уполномоченные ИТ-сотрудники из информационно-технических служб и служб разработки и эксплуатации систем. Руководство CSIRT состоит из главного специалиста информационной службы (Chief Information Officer), начальника службы безопасности (Chief of Police), директора государственной информации (Director of Public Information), директора службы информационных технологий (Director of Information Technology Services), директора отдела разработки и эксплуатации систем (Director of Systems Development and Maintenance), CISO, менеджера по обслуживанию систем и сетей, юридического консультанта, советника по кадрам и делегатов с техническими экспертными знаниями, специально назначенных вице-президентами.

Персонал **Отдела службы информационных технологий** включает администраторов и инженеров по обслуживанию систем и сетей, а также поставщиков технических услуг, таких как: сервисная служба ИТ (IT Help Desk), специалистов по технической поддержке пользователей и администраторов по обслуживанию голосовых сообщений. Они отвечают за объединение технических средств по обеспечению информационной безопасности, средств управления и практики работы в сетевой среде. Они получают сообщения о подозрительных сбоях в системе информационной безопасности или об инцидентах от конечных пользователей.

В состав персонала **Отдела разработки и обслуживания систем** входят разработчики и администраторы баз данных. Они разрабатывают, используют, интегрируют и внедряют передовой опыт в области безопасности для государственных приложений, а также обучают разработчиков веб-приложений применению принципов обеспечения безопасности.

Другие

Сотрудники, имеющие доступ к информации и информационным системам, должны соответствовать применяемой государственной политике и процедурам, а также любым дополнительным методам или процедурам, установленным руководителями или директорами своих подразделений. Это включает в себя защиту паролей своих учетных записей и информирование соответствующей стороны (как правило, своего руководителя) о возможном неправомерном использовании информации или об инцидентах в области информационной безопасности.

Временные сотрудники считаются работниками и имеют те же обязанности, что и сотрудники, занятые на полный или неполный рабочий день, в отношении доступа к информации и информационным системам.

Консультанты, поставщики услуг и другие третьи стороны, работающие по контракту, имеют доступ к информации на основе «принципа необходимого знания». Сетевые учетные записи, необходимые третьей стороне, должны запрашиваться «поручителем» из организации, который следит за тем, что пользователь третьей стороны понимает отдельные функции относительно сетевой учетной записи, и который утвержден соответствующим вице-президентом или директором. Пользователь должен хранить свой пароль(-и) в безопасности и нести ответственность за любые действия, исходящие от использования его/ее идентификатора пользователя в разумных рамках контроля с его/ее стороны.

3. Создание рамочной структуры политики в области информационной безопасности

Рамочная структура в области информационной безопасности

Рамочная структура по информационной безопасности устанавливает параметры для политики в области информационной безопасности. Это гарантирует, что данная политика принимает во внимание ресурсы в области ИТ (люди, информационные документы, аппаратные средства, программное обеспечение, услуги); отражает международные права и нормы; и отвечает принципам информационной доступности, конфиденциальности, целостности, ответственности и гарантии. Рисунок 22 показывает рамочную структуру по информационной безопасности.

Рисунок 22. Рамочная структура по информационной безопасности

Политика в области информационной безопасности является наиболее важной частью рамочной структуры по информационной безопасности. Политика включает в себя пять направлений, которые рассматриваются ниже.

а. Планирование и организация: Эта область включает в себя обеспечение безопасности организации и работы, а также классификацию активов и контроль.

Обеспечение безопасности организации и работы охватывает **—**

- Организацию и систему государственной организации по обеспечению информационной безопасности
- Порядок действий каждой организации по обеспечению информационной безопасности
- Устройство и управление информационной безопасностью страны
- Сотрудничество с соответствующим международным агентством
- Сотрудничество с экспертной группой

Классификация активов и контроль включает в себя —

- Предоставление в собственность и стандартизацию классификации для важных информационных активов
- Инструкцию по регистрации и оценке степени риска для важных информационных активов
- Управление правами доступа к важным информационным активам
- Публикацию и передачу важных информационных активов
- Переоценку и расходование важных информационных активов
- Управление безопасностью документов

б. Приобретение и внедрение: Данная область включает в себя безопасность при решении кадровых вопросов, приобретение информационных систем и обеспечение безопасности разработок.

Безопасность при решении кадровых вопросов предполагает определение метода управления для найма новых сотрудников, что включает в себя **—**

- Меры противодействия по безопасности человеческих ресурсов и подготовку по вопросам безопасности
- Обработку нарушения норм и правил безопасности
- Управление системой безопасности при доступе третьих сторон
- Управление системой безопасности при доступе внешнего персонала
- Работу и управление третьими лицами и сотрудниками со стороны
- Управление безопасностью компьютерного помещения и оборудования
- Доступ к основным помещениям и зданиям
- Обработку происшествий по безопасности

Приобретение информационных систем и обеспечение безопасности разработок требует —

- Проверки безопасности при приобретении информационной системы
- Управления безопасностью при внутреннем и внешнем применении программ
- Государственной системы шифрования (программу и ключ шифрования и так далее)
- Испытаний после разработки программы

- Рекомендуемых требований по безопасности в случае разработки вне организации
- Контроля безопасности в процессе разработки и приобретения

в. **Защита неприкосновенности частной жизни:** Включение защиты неприкосновенности частной жизни в политику информационной безопасности не является обязательным. Однако введение такой защиты является преимуществом, так как защита неприкосновенности частной жизни является международной проблемой. Обеспечение защиты неприкосновенности частной жизни должно охватывать следующее —

- Сбор и использование персональной информации
- Предварительное согласие, когда частная жизнь людей используется в чьих-либо интересах
- PIA

г. **Эксплуатация и поддержка:** Данная область имеет отношение к физической и технической безопасности, когда использование сети и системы регулируется в деталях, а физическая безопасность информации и инфраструктуры коммуникации заранее определена.

Эксплуатация информационной системы и управление безопасностью включает определение следующего —

- Эксплуатация и управление безопасностью сервера, сети, приложений и базы данных
- Разработка системы обеспечения информационной безопасности
- Регистрация и резервная копия в случаях судебного иска
- Управление хранением информации
- Мобильные вычисления
- Стандарт для хранения и безопасности компьютерных данных
- Услуги электронной коммерции

Управление безопасностью доступа к учетной записи - Контроль доступа и управление учетной записью должны быть определены для обеспечения конфиденциальности в использовании национального информационного хранилища. Это включает в себя —

- Регистрацию, удаление, управление правом доступа пользователей национальной информационной системы
- Учетную запись и управление правом доступа зашифрованной компьютерной сети

Физическая безопасность – Физическая безопасность относится к защите информации и средств связи, которые содержат важную информацию. Она включает в себя —

- Методы настройки и управления областью безопасности
- Контроль доступа и транспортировки к компьютерному центру
- Предотвращение ущерба от стихийных и других бедствий

д. **Мониторинг и оценка:** Данная область политики по информационной безопасности требует разработки стандартов и процедур для предотвращения инцидентов в области безопасности, а также управления и реагирования на инциденты безопасности.

Проверка безопасности включает в себя —

- Создание плана проверки безопасности
- Осуществление периодической проверки безопасности
- Составление/организацию форм отчетов
- Определение субъекта проверки безопасности и целей отчета

Управление и реагирование на инциденты безопасности требует определения—

- Работы и роли каждой организации в обработке инцидентов, связанных с безопасностью
- Процедур наблюдения и распознавания признаков инцидентов в области безопасности
- Процедуры обработки инцидента безопасности и метода реагирования
- Принятия мер после обработки инцидента в области безопасности

4. Учреждение и/или пересмотр законов в соответствии с политикой в области информационной безопасности

Законы должны соответствовать политике в области информационной безопасности. Должны быть законы, регулирующие государственные организации и частные предприятия. В таблицах 14-16 перечислены законы, связанные с вопросами по информационной безопасности, в Японии, ЕС и США соответственно. В Японии главным законом в сфере ИТ является основной закон по формированию сетевого общества, применяющего передовую информацию и телекоммуникации (Basic Act on the Formation of an Advanced Information and Telecommunications Network Society). Данный закон является основным стандартом для информационной безопасности в стране, и все связанные законы должны соответствовать ему.

Таблица 14. Соответствующие законы по вопросам обеспечения информационной безопасности в Японии

Законы	Целевая отрасль	Цель регулирования	Взыскание
Закон о неправомерном компьютерном доступе	Все отрасли	Действие, которое способствует неправомочному доступу и передаче чужой информации без предварительного уведомления	
Акт по защите персональной информации	Частные предприятия, использующие персональную информацию в коммерческих целях	Управление частной информацией (адрес, телефон, e-mail и др.)	Уголовная ответственность, штраф
Акт об электронной подписи и сертификации		Упрощение электронной торговли, которая использует в своих интересах Интернет и экономическую деятельность на основе сетей	

Таблица 15. Законы, связанные с информационной безопасностью в ЕС

Законы	Подробности
Единая нормативно-правовая база (Директива 2002/21/EC)	• Представляет основу по регулированию телекоммуникационных сетей и услуг • Направлена на защиту неприкосновенности частной жизни путем обеспечения безопасных коммуникационных сетей
Директива ЕС о защите данных (Директива 1995/46/EC)	• Руководство по обработке и бесплатному удалению персональной информации • Основной закон, определяющий ответственность стран-членов и признающий верховную власть индивидуумов на персональную информацию • Более строгий, чем стандарт США
Директива ЕС об электронных подписях (Директива 1999/93/EC) Директива ЕС об электронной коммерции (Директива 2000/31/EC)	• Регулирует применение электронных подписей • Регулирует ведение электронной коммерции
Договор о киберпреступности	• Наиболее всеобъемлющий международный договор о киберпреступности; • Определяет в деталях все преступные действия, которые используют Интернет, и соответствующие им меры наказания
Руководство по защите данных в коммуникациях и сетях	• Требует от поставщиков коммуникационных услуг сохранять данные о звонках от 6 до 24 месяцев (обнародовано после террористических атак в Мадриде и Лондоне в 2004 и 2005гг.)

Таблица 16. Законы, связанные с информационной безопасностью в США

Законы	Целевая отрасль	Цели регулирования	Взыскание
Федеральный закон об управлении информационной безопасностью 2002 г.	Федеральные административные учреждения	Информация об административных учреждениях, системах в области ИТ, программах по обеспечению информационной безопасности	-
Закон о преемственности страхования и отчетности в области здравоохранения от 1996 г.	Медицинские учреждения и поставщики медицинских услуг	Электронные данные по персональной медицинской информации	Уголовная ответственность, штраф
Закон Грэмма-Лича-Блилей от 1999 г.	Финансовые институты	Частная информация клиентов	Уголовная ответственность, штраф
Закон Сарбаниса-Оксли от 2002 г.	Список компаний Фондовой биржи США	Внутренний контроль и открытые финансовые отчеты	Уголовная ответственность, штраф
Закон о повреждении информации и защите базы данных Калифорнии от 2003 г.	Административные учреждения и частные предприятия Калифорнии	Зашифрованная частная информация	Штраф и извещение пострадавшего

5. Распределение бюджета для осуществления информационной политики

Осуществление политики требует финансовых средств. Таблица 17 показывает расходы по обеспечению информационной безопасности в Японии и США за последние годы.

Таблица 17. Расходы по защите информации в Японии и США

Япония	**2004**	**2005**
Общий годовой бюджет	848,967,000 000 000 яп. йен	855,195,000,000,000 яп. йен
Бюджет по обеспечению информационной безопасности	267,000,000,000 яп. йен	288,000,000,000 яп. йен
Процент от общего бюджета	0.03%	0.03%
США	**2006**	**2007**
Общий годовой бюджет	2,709,000,000,000 долл.США	2,770,000,000,000 долл.США
Бюджет по обеспечению информационной безопасности	5,512,000,000 долл.США	5,759,000,000 долл.США
Процент от общего бюджета	0.203%	0.208%

Практическое упражнение

Если в вашей стране проводится политика по обеспечению информационной безопасности, проследите ее развитие с точки зрения пяти аспектов разработки политики в области информационной безопасности, описанных выше. То есть, опишите:

1. Курс политики
2. Организацию по обеспечению информационной безопасности
3. Политическую рамочную структуру
4. Законы, поддерживающие политику по обеспечению информационной безопасности
5. Бюджетное распределение для обеспечения информационной безопасности

Если в вашей стране еще не проводится политика обеспечения информационной безопасности, обрисуйте в общих чертах некоторые возможности для каждого из этих пяти аспектов, приведенных выше, по отношению к формулированию политики. Используйте следующие вопросы в качестве облегчения данного упражнения:

1. Какой должен быть курс политики по обеспечению информационной безопасности в вашей стране?
2. Какая организационная структура должна быть учреждена? Какие организации должны быть вовлечены в разработку и внедрение политики по обеспечению информационной безопасности в вашей стране?
3. Какие конкретные вопросы должна охватывать политическая рамочная структура?
4. Какие законы должны быть приняты и/или отменены в поддержку информационной политики?
5. Какие бюджетные соображения следует принять во внимание? Как должен быть составлен бюджет?

Участники, прибывшие из одной страны, могут выполнять данное упражнение в группе.

7.3 Исполнение/внедрение политики

Беспрепятственное осуществление политики по обеспечению информационной безопасности требует сотрудничества между государственными, частными и международными кругами. Рисунок 23 показывает определенные направления осуществления информационной политики, где сотрудничество имеет решающее значение.

Рисунок 23. Области для сотрудничества при осуществлении политики по обеспечению информационной безопасности

Разработка политики по обеспечению информационной безопасности

Таблица 18 представляет, каким образом правительство, частный сектор и международные организации могут способствовать разработке национальной политики по обеспечению информационной безопасности.

Таблица 18. Сотрудничество при разработке политики по обеспечению информационной безопасности (пример)

Сектор	Вклад в разработку политики
Правительство	• Организация по разработке национальной стратегии и планированию: обеспечение соответствия между информационной политикой и национальным планом • Организация по информационным и коммуникационным технологиям: обеспечение сотрудничества учреждений по стандартам в области государственной безопасности информационных технологий • Организация по анализу тенденций развития информационной безопасности: отражение отечественных и международных тенденций и анализа при разработке политики • Организация по правовому анализу: проверка соответствий между политикой по обеспечению информационной безопасности и действующим законодательством • Национальная информационная организация: сотрудничество при создании и выборе направления стратегии • Следственные учреждения: сотрудничество при устранении инцидентов безопасности
Частный сектор	• Консалтинговые компании по информационной безопасности: использование профессиональных агентов в разработке политики по обеспечению информационной безопасности • Лаборатория технологий безопасности персональной информации: создание технологических стандартов, связанных с информационной безопасностью • Департаменты по информационной безопасности университетов и/или колледжей: обеспечение экспертной оценки при разработке политики
Международные организации	• Обеспечение соответствия международным стандартам политики • Координация реагирования на международные угрозы и аварийные ситуации

Управление и защита информационной и коммуникационной инфраструктуры

Эффективное использование (сбор, хранение и т.д.) информации требует надлежащего управления и защиты инфраструктуры в области ИТ. Хорошая политика по обеспечению информационной безопасности бесполезна в отсутствии надежной ИТ-инфраструктуры.

Эффективное управление и защита информационной и коммуникационной инфраструктуры требуют сотрудничества между менеджерами в области сети, систем и ИТ. Кроме того, достигается хороший эффект в случае сотрудничества между государственными учреждениями и частными организациями (Таблица 19).

Таблица 19. Сотрудничество в области управления и защиты информационной и коммуникационной инфраструктуры (пример)

Сектор	Вклад в управлении и защите информационной и коммуникационной инфраструктуры
Правительственный сектор	• Организация, имеющая отношение к информационным и коммуникационным сетям: определение состава и уровня безопасности национальной и коммуникационной сети • Лаборатория по информационным и коммуникационным технологиям: распространение государственных стандартов и заимствование применимых технологий
Частный сектор	• Поставщик услуг Интернет: сотрудничество в формировании национальной информационной и коммуникационной сети • Лаборатория по информационным и коммуникационным технологиям: обеспечение услуг технического развития, а также сотрудничество по обеспечению стабильной информационной и коммуникационной инфраструктуры и технологий безопасности
Международные организации	• Сотрудничество с международными организациями по технологическим стандартам для международного обмена информацией и коммуникациям, а также для защиты новых информационных технологий

Предотвращение и реагирование на угрозы и инциденты

Эффективное реагирование на угрозы и нарушения информационной безопасности требует сотрудничества между национальной информационной организацией, следственными органами и правовыми институтами, а также организациями, которые проводят инспекцию аварий безопасности и оценку ущерба. Кроме того, крайне важно сотрудничать с организацией, которая может проанализировать технические уязвимости и назначить технические меры противодействия.

Таблица 20. Сотрудничество по реагированию на аварии информационной безопасности (пример)

Сектор	Вклад
Государственные организации	• Организация по реагированию на инциденты безопасности: обеспечение ситуационного анализа, реагирования на инцидент взлома, а также технологии реагирования на нарушения и аварии • Национальная информационная организация: анализ и проверка нарушений и аварий, имеющих отношение к информационной безопасности • Следственные учреждения: сотрудничество с организацией, вовлеченной в деятельность по задержке и преследованию нарушителей • Организация, предоставляющая оценку безопасности: подтверждение безопасности и надежности информационной сети и производства на основе информационной безопасности • Организация по обучению информационной безопасности: анализ причин аварий информационной безопасности и просвещение населения в целях предотвращения повторения аварий
Частные группы	• Организация по реагированию на частные инциденты: обеспечение реагирования и технической поддержки • Частные следственные организации: сотрудничество с государственными следственными органами
Международные организации	• Уведомление и сотрудничество с Интерполом и CERT/CC в случаях международных угроз и инцидентов

Предотвращение инцидентов информационной безопасности

Предотвращение нарушений и аварий информационной безопасности включает в себя мониторинг, обучение и управление изменениями. Национальная CSIRT является основной организацией по мониторингу. Критическая область заключается в обеспечении соответствия информационной политики с реальными данными мониторинга. Таким образом, необходимо обсудить масштабы мониторинга информационной политики. Кроме того, важно обучить сотрудников государственных и частных организаций, а также широкую общественность политике по обеспечению информационной безопасности. Может оказаться необходимым изменить некоторые подходы к информации и формы поведения, которые оказывают влияние на информацию по вопросам безопасности. Обучение информационной безопасности и управление изменениями определены в документе US SP 800-16 (Требования по подготовке кадров в области обеспечения безопасности информационных технологий).

Таблица 21. Сотрудничество в предотвращении нарушений и аварий в области информационной безопасности (пример)

Сектор	Координирование
Государственные организации	• Агент по мониторингу: непрерывный мониторинг сети и раннее обнаружение угроз безопасности • Агент по сбору: обмен информацией с международными организациями и сайтами по безопасности • Учебное заведение: периодическое моделирующее обучение для развития способностей и возможностей быстрого реагирования на нарушения и аварии в области информационной безопасности
Частные организации	• Поставщик услуг Интернет, компании по контролю безопасности и производству антивирусных программ: предоставление статистики трафика, информации по типам атак и сведений о «червях»/вирусах
Международные организации	• Предоставление информации по типам атак, сведений о «червях»/вирусах и тому подобное

Безопасность неприкосновенности частной жизни

Сотрудничество необходимо для установления мер по защите неприкосновенности частной жизни в Интернете, предотвращению инцидентов по вопросам частной информации определения местонахождения, защите частной биологической информации и отчетности о нарушениях неприкосновенности частной жизни.

Таблица 22. Координация по защите неприкосновенности частной жизни (пример)

Сектор	Координация
Государственные агентства	• Организация по системному анализу: ведение деятельности, связанной с частной информацией определения местонахождения, а также анализа в области тенденций защиты внутренней и внешней личной информации • Организация по планированию: усовершенствование законов/систем, технических/административных мер и управление стандартами • Техническая поддержка: координирование сертификации компьютерного пользователя для предприятий • Организация услуг: координирование поддержки по устранению нарушений неприкосновенности частной жизни и случаев спама
Частные организации	• Организация по безопасности персональной информации: регистрация требований и организация совместных ассоциаций по обеспечению безопасности персональной информации • Консалтинг по вопросам обеспечения безопасности персональной информации
Международные организации	• Сотрудничество по применению международных стандартов по безопасности персональной информации

Международная координация

Информационная безопасность не может быть достигнута только усилиями одной страны, потому что нарушения информационной безопасности, как правило, происходят в международных масштабах. Таким образом, международная координация по защите информационной безопасности в государственном, а также в частном секторе должна быть институционально оформлена и наделена законным статусом.

Для частного сектора соответствующей международной организацией по содействию и защите информационной безопасности является CERT/CC. Для правительственного уровня ENISA (для ЕС) и МСЭ стремятся развивать сотрудничество по информационной безопасности между странами.

В каждой стране должно быть государственное учреждение, роль которого состоит в способствовании сотрудничества государственных и частных организаций с международными организациями и учреждениями.

Практическое упражнение

1. Определите государственные учреждения и частные организации в вашей стране, которые должны взаимодействовать и сотрудничать в осуществлении национальной политики по обеспечению информационной безопасности. Определите также международные организации, с которыми они должны координировать свою деятельность.

2. Для каждой области сотрудничества при выполнении информационной политики, показанной на рисунке 23, определите конкретные меры или мероприятия, которые могут предпринять данные агентства и организации.

Участники, прибывшие из одной страны, могут выполнить данное упражнение в группе.

7.4 Обзор и оценка политики по обеспечению информационной безопасности

Заключительным шагом при разработке политики по обеспечению информационной безопасности является оценка политики и внесение дополнений в недостаточно проработанные части. Пересмотр политики является существенным после того, как определяется эффективность политики по обеспечению информационной безопасности.

Метод оценки внутренней политики может применяться для определения эффективности национальной политики по обеспечению информационной безопасности. Аспекты данного метода рассматриваются ниже.

Использование аудиторских организаций

Существуют организации, чья роль заключается в проведении экспертизы и оценки политики. Такая организация должна проводить регулярные ревизии национальной политики в области обеспечения информационной безопасности. Кроме того, эта организация должна быть независимой от организаций, разрабатывающих и внедряющих политику по обеспечению информационной безопасности.

Пересмотр политики по обеспечению информационной безопасности

Проблемные области, как правило, выявляются во время ревизии политики. В этом случае необходим порядок пересмотра политики для решения данных проблемных участков.

Изменения в среде

Чуткое реагирование на изменения в политической среде считается очень важным. Изменения, вытекающие из международных угроз (атак) и уязвимостей, изменения в ИТ-инфраструктуре, оценка изменений в критически важной информации и другие важные изменения такого рода должны быть сразу же отражены в национальной политике по обеспечению информационной безопасности.

Проверьте себя

1. Как различные этапы жизненного цикла политики в области обеспечения информационной безопасности воздействуют друг на друга? Можно ли пропустить этапы? Почему да или почему нет?

2. Почему сотрудничество между различными секторами важно при разработке и осуществлении политики обеспечения информационной безопасности?

ПРИЛОЖЕНИЕ

Дополнительная литература

Butt, Danny, ed. 2005. *Internet Governance: Asia-Pacific Perspectives*. Bangkok: UNDP-APDIP. http://www.apdip.net/publications/ict4d/igovperspectives.pdf.

CERT. CSIRT FAQ. Carnegie Mellon University. http://www.cert.org/csirts/csirt_faq.html.

CERT. Security of the Internet. Carnegie Mellon University. http://www.cert.org/encyc_article/tocencyc.html.

Dorey, Paul and Simon Perry, ed. 2006. *The PSG Vision for ENISA*. Permanent Stakeholders Group. http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

ESCAP. Module 3: Cyber Crime and Security. http://www.unescap.org/icstd/POLICY/publications/internet-use-for-business-development/module3-sources.asp.

Europa. Strategy for a secure information society (2006 communication). European Commission. http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

Information and Privacy Office. 2001. *Privacy Impact Assessment: A User's Guide*. Ontario: Management Board Secretariat. http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Information Security Policy Council. *The First National Strategy on Information Security*. 2 February 2006. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

ISO. ISO/IEC27001:2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.

ITU and UNCTAD. 2007. Challenges to building a safe and secure Information Society. In *World Information Society Report 2007*, 82-101. Geneva: ITU. http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/report.html.

ITU-D Applications and Cybersecurity Division. ITU National Cybersecurity / CIIP Self-Assessment Tool. ITU. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Killcrece, Georgia. 2004. *Steps for Creating National CSIRTs*. Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek. 2003. *Organizational Models for Computer Security Incident Response Teams (CSIRTs).* Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive/pdf/03hb001.pdf.

OECD. 2002. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Paris: OECD. http://www.oecd.org/dataoecd/16/22/15582260.pdf.

OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Shimeall, Tim and Phil Williams. 2002. *Models of Information Security Trend Analysis*. Pittsburgh: CERT Analysis Center. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.

The White House. 2003. *The National Strategy to Secure Cyberspace*. Washington, D.C.: The White House. http://www.whitehouse.gov/pcipb.

Заметки для инструктора

Как было отмечено в разделе, озаглавленном как «О серии учебных модулей», данный и другие модули серии призваны для того, чтобы представлять ценность для различных слушателей в разнообразных и изменяющихся национальных условиях. Эти модули разработаны таким образом, чтобы быть представленными полностью или по частям, в различных режимах – как в режиме реального времени, так и автономно. Модуль может изучаться отдельными учащимися и группами учащихся в учебных заведениях, а также в рамках государственных учреждений. Уровень участников и продолжительность учебных занятий будет определять объем детализации представления информации.

Данные заметки предлагают вниманию инструкторов некоторые идеи и предложения по более эффективному представлению информации модуля.

Дальнейшие указания по учебным подходам и стратегиям представлены в справочнике по разработке учебных программ, разработанного в качестве сопутствующего материала для *Академии ИКТ для лидеров государственного управления*. Руководство доступно по адресу: http://www.unapcict.org/academy.

Структурирование занятий

Для занятия продолжительностью 90 минут

Обеспечение краткого обзор основных понятий и международных стандартов или принципов в области информационной безопасности и защиты неприкосновенности частной жизни (разделы 1 и 5 настоящего модуля). Подчеркните необходимость в соответствующей и эффективной политики по обеспечению информационной безопасности и защиты неприкосновенности частной жизни.

Для занятий продолжительностью 3 часа

Разделите занятие на две части. В первой части рекомендуется сосредоточить внимание на основных концепциях и тенденциях в области информационной безопасности, в том числе описание анализа тенденций угроз информационной безопасности (раздел 2). Во второй части стоит уделить внимание основным концепциям и принципам защиты неприкосновенности частной жизни, способствовать обсуждению вопросов, которые влияют на защиту неприкосновенности частной жизни, и кратко описать оценку воздействия на неприкосновенность частной жизни.

Для занятий продолжительностью один день (6 часов)

После краткого обзора основных концепций и принципов в области информационной безопасности и защиты неприкосновенности частной жизни необходимо сосредоточить внимание на разработке и осуществлении политики по обеспечению информационной безопасности (раздел 7). Здесь можно начать с опроса участников о политических последствиях данных принципов информационной безопасности и защиты неприкосновенности частной жизни. Затем, прежде чем перейти к процессу разработки политики, кратко представить жизненный цикл политики по обеспечению информационной безопасности. Участникам из стран с существующей политикой по обеспечению информационной безопасности можно предложить оценить эту политику с точки зрения рассмотренных принципов и процедур, в то время как участникам из стран, не имеющих

политику по обеспечению информационной безопасности, можно предложить изложить в общих чертах некоторые аспекты такой политики (см. практическое упражнение в конце раздела 7.2).

Для занятия продолжительностью два дня

Первый день может быть проведен, как описано выше, а второй день можно провести, уделив внимание деятельности и методологии по обеспечению информационной безопасности (разделы 3 и 4), в частности, созданию CSIRT (раздел 6). Можно рассмотреть примеры из других стран, и следует поощрить участников на определение наиболее подходящей модели CSIRT и разработку конкретных механизмов вмешательства по обеспечению безопасности, исходя из своих собственных национальных условий.

Интерактивность

Очень важно взаимодействовать с аудиторией и выполнять практические упражнения. Данный модуль предоставляет много полезной информации, но участники обучения должны быть в состоянии критически анализировать эту информацию и применять ее там, где целесообразно это сделать. В модуле приводятся некоторые тематические исследования, которые следует обсудить, когда это возможно, с точки зрения понятий и принципов по обеспечению информационной безопасности. Однако участников следует также подвигнуть к изучению аутентичных вопросов и проблем в области информационной безопасности и защиты неприкосновенности частной жизни, исходя из своих собственных условий.

О KISA

Корейское агентство по информационной безопасности (Korea Information Security Agency, KISA) было создано правительством в 1996 году в качестве центра передового опыта, отвечающего за общенациональное содействие эффективной разработки политики по укреплению информационной безопасности. В его функции входят предупреждение и реагирование на нарушения в Интернете, ответ на спам, защита неприкосновенности частной жизни, проверка электронной подписи, защита критической инфраструктуры, оценка безопасности для продуктов информационной безопасности и отраслевой поддержки, всестороннее развитие политики и технологий, а также повышение уровня осведомленности в направлении создания безопасного и надежного информационного общества.

АТУЦ ИКТР

Азиатско-Тихоокеанский учебный центр информационных и коммуникационных технологий для развития при ООН является вспомогательным органом Экономической и социальной комиссии ООН для Азии и Тихого океана (ЭСКАТО). Целью АТУЦ ИКТР является активизация усилий стран-членов ЭСКАТО по использованию ИКТ в их социально-экономическом развитии на основе создания человеческого и институционального потенциала. Работа АТУЦ ИКТР сосредоточена на трех основных компонентах:

1. Обучение. Для повышения знаний и навыков в области ИКТ разработчиков политики и ИКТ-специалистов, а также укрепление потенциала инструкторов и учебных заведений в области ИКТ;
2. Исследование. Для проведения аналитических исследований, связанных с развитием человеческих ресурсов в области ИКТ;
3. Консультации. Для оказания консультационных услуг по программам развития человеческих ресурсов для членов и ассоциированных членов ЭСКАТО.

АТУЦ ИКТР находится в г. Инчон, Республика Корея.

http://www.unapcict.org

ЭСКАТО

ЭСКАТО является региональным подразделением Организации Объединенных Наций и выступает в качестве главного центра ООН экономического и социального развития в Азиатско-Тихоокеанском регионе. Ее задача заключается в укреплении сотрудничества между ее 53 членами и 9 ассоциированными членами. ЭСКАТО обеспечивает стратегическую связь между глобальными и программами и проблемами на национальном уровне. Она оказывает поддержку правительствам стран региона в деле укрепления региональных позиций и защищает региональные подходы в решении уникальных социально-экономических проблем в условиях глобализации в мире. ЭСКАТО находится в Бангкоке, Таиланд.

http://www.unescap.org

Серия модулей Академии ИКТ для лидеров государственного управления

http://www.unapcict.org/academy

Академия представляет собой всеобъемлющую учебную программу в области ИКТР, состоящую из восьми модулей, основная цель которых оснастить разработчиков политики необходимыми знаниями и навыками по использованию в полной мере возможностями ИКТ для достижения целей национального развития и преодоления «цифрового разрыва».

Модуль 1 – Взаимосвязь между ИКТ и полноценным развитием

Освещаются ключевые вопросы и решения от этапов создания политики до реализации в области использования ИКТ для достижения Целей развития тысячелетия.

Модуль 2 –Политика, процессы и управление ИКТ в целях развития

Основное внимание уделяется вопросам создания политики и управления ИКТР, а также предлагается важная информация об аспектах национальной политики, стратегий и рамочных структур, способствующих ИКТР.

Модуль 3 – Применение электронного правительства

Изучаются концепции электронного правительства, принципы и виды приложений. Здесь также рассматриваются вопросы построения систем электронного правительства и определения соображений процесса проектирования.

Модуль 4 – Тенденции развития ИКТ

Содержится анализ современных тенденций в области ИКТ и будущих направлений развития. Здесь также рассматриваются основные технические и политические соображения при принятии решений в области ИКТР.

Модуль 5 – Управление использованием Интернета

Рассматривается дальнейшее развитие международной политики и процедур, которые регулируют использование и эксплуатацию сети Интернет.

Модуль 6 – Обеспечение информационно-сетевой безопасности и неприкосновенности частной жизни

Рассматриваются вопросы и тенденции в области информационной безопасности, а также процесс разработки стратегии по обеспечению информационной безопасности.

Модуль 7 – Управление проектами в области ИКТ в теории и на практике

Представляются концепции управления проектами, имеющими отношение к проектам в области ИКТР, в том числе широко используемые методы, процессы и порядки в области управления проектами.

Модуль 8 – Варианты финансирования ИКТ в целях развития

Изучаются варианты финансирования проектов в области ИКТР и электронного правительства. Освещается государственно-частное партнерство, как особо полезного варианта финансирования в развивающихся странах.

В настоящее время данные модули дополнены местными тематическими исследованиями национальными партнерами Академии для обеспечения значимости модулей и удовлетворения потребностей разработчиков политики в разных странах. Эти модули также переведены на разные языки. Кроме того, данные модули будут регулярно обновляться в целях обеспечения их актуальности для разработчиков политики, а также для разработки новых модулей, направленных на ИКТР 21-го века.

Виртуальная академия АТУЦ ИКТР (AVA – http://ava.unapcict.org)

- Интернет-платформа дистанционного обучения для *Академии*.
- Разработана для обеспечения доступности в режиме онлайн всех модулей Академии, включая виртуальные лекции, презентации и тематические исследования.
- Предоставляет возможность обучающимся лицам изучать материалы по своему усмотрению.

Электронный центр ИКТР для совместной работы (e-Co Hub – http://www.unapcict.org/ecohub)

- Ресурсный и сетевой портал для обмена знаниями в области ИКТР.
- Предоставляет удобный доступ к содержанию модулей.
- Пользователи могут участвовать в дискуссиях в режиме онлайн и стать частью Интернет-собщества практиков e-Co Hub, которая служит для обмена опытом и расширения базы знаний в области ИКТР.

Чтобы в полной мере воспользоваться услугами, предоставляемыми AVA и e-Co Hub, зарегистрируйтесь по следующему адресу: http://www.unapcict.org/join_form

Серия модулей Академии ИКТ для лидеров государственного управления

Модуль 6: Обеспечение информационно-сетевой безопасности и неприкосновенности частной жизни

Перевод с английского
под редакцией А.С. Бакенова

Бумага офсетная. Гарнитура Arial
14,42 печ. л. Тираж: 200 экз.

Верстка осуществлена М. Усубалиевой

Дизайн и разметка: Scandinavian Publishing Co., Ltd and studio triangle

Отпечатано в Национальном центре информационных технологий Кыргызской Республики и ОсОО ИК «Zest-Asia»