

1 Характеристика международных организаций в сфере управления информационной безопасностью

В числе международных организаций, действующих в сфере управления информационной безопасностью и оказывающих существенное влияние на функционирование глобальных информационных систем и деятельность всего информационного сообщества, выделяются организации следующих типов.

1) Крупные международные некоммерческие и неправительственные организации, объединяющие специалистов в определенных областях, существующие, как правило, уже в течение многих лет и охватывающие множество основных направлений развития компьютерной инженерии, электроники и телекоммуникаций, включая, в том числе и определенные вопросы обеспечения безопасности современных информационных технологий.

2) Отдельные относительно небольшие организации, которые специализируются на более или менее узких вопросах информационной безопасности, имеющих глобальное значение для всего сообщества пользователей информационных систем, и появились на базе частных компаний или исследовательских структур в течение последнего десятилетия, когда проблемы информационной безопасности стали особенно актуальными.

3) Совместные структуры (комитеты, альянсы и др.), создаваемые (иногда временно) крупными компаниями (иногда при участии крупных исследовательских центров, учебных заведений и правительственных структур) для решения определенных задач в сфере информационных технологий и информационной безопасности.

Каждый из типов организаций, в свою очередь, имеет свои специфические организационные особенности, однако все они, как правило,

Тема 3.1 – Международные организации планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

решают задачу разработки, согласования и дальнейшего распространения, общих для всего сообщества пользователей информационных систем технических и организационных решений, таких как:

- протоколы глобальных сетей;
- архитектуры, алгоритмы, протоколы публичных средств шифрования данных;
- правила построения глобальных сетей обмена данными и других элементов глобальной инфраструктуры информационной безопасности.

Также важными элементами организационной работы на уровне международных структур являются:

- организация обмена знаниями и актуальными новостями в среде специалистов по информационной безопасности в таких формах, как публикация специализированных периодических изданий и сборников научных работ, организация специализированных научно-практических конференций, семинаров и др.;
- организация и поддержание в актуальном состоянии баз данных и баз знаний, которые содержат сведения, необходимые пользователям информационных систем, администраторам, разработчикам и другим участникам для обеспечения информационной безопасности.

Примерами таких баз данных являются базы данных, содержащие сведения о выявленных уязвимостях различных программных и аппаратных платформ информационных систем.

В целом организационная работа на уровне международных структур не является универсальной, и в большинстве случаев они строят свою работу самостоятельно. Однако можно выделить некоторые основные организационные принципы, характерные для деятельности многих из них:

1) Принцип добровольности участия в работе таких структур и в отдельных проектах или во всей работе.

2) Принцип открытости (доступности) результатов работы (всех или их части) для сообщества специалистов в сфере информационных технологий.

3) Принцип самофинансирования.

Работа крупных международных профессиональных (отраслевых) организаций (объединений), как правило, имеет следующие отличительные особенности:

1) Она, как правило, не направлена только на решение задач информационной безопасности – задачи информационной безопасности решаются в комплексе со множеством других проблем (развития информационных технологий, построения телекоммуникационных систем и др.).

2) Она в определенной мере может опираться на поддержку со стороны различных государственных структур.

3) Она объединяет большое количество специалистов из различных исследовательских, учебных, коммерческих организаций, но при этом большинство участников (членов) может не иметь конкретных обязательств, обязывающих вносить вклад в работу и достигать определенных целей.

2 Международные профессиональные объединения управления информационной безопасностью

Основными наиболее крупными и известными международными профессиональными объединениями, так или иначе связанными с вопросами информационной безопасности, являются:

- ITU – International Telecommunication Union;
- IEEE – Institute of Electrical and Electronics Engineers;
- ACM – Association for Computing Machinery;

Тема 3.1 – Международные организации планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

- W3 Consortium;
- ISSA – Information Systems Security Association;
- ISO – International Organization for Standardization;
- IETF – Internet Engineering Task Force;
- ICISA – International Computer Security Association;
- Information Systems Audit and Control Association (ISACA);
- Internet Security Alliance.

2. 1 Международный союз электросвязи

International Telecommunication Union (ITU) – Международный союз электросвязи является старейшей международной организацией, связанной с информационными технологиями. Она была основана в 1885 году как Международный телеграфный союз и получила свое новое название в 1934 году. В настоящее время ITU объединяет 189 государств. Как понятно из названия, основной ее задачей изначально было управление и координация деятельности в сфере передачи информации и, в частности, в радиосвязи и телеграфной связи. Однако по мере развития глобальных компьютерных сетей и интеграции компьютерных и телекоммуникационных систем, область деятельности ITU была значительно расширена и в настоящее время включает в себя множество вопросов, связанных с построением компьютерных сетей, передачей цифровых данных, обработкой информации и др.

Членами ITU-T являются:

- государственные органы власти (министерства и ведомства связи отдельных стран);
- научные организации и компании – производители телекоммуникационного оборудования;
- региональные и международные телекоммуникационные организации.

Тема 3.1 – Международные организации планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

Функциональными органами ITU-T являются:

- Всемирная ассамблея по стандартизации телекоммуникаций (World Telecommunication Standardization Assembly), проводимая каждые четыре года, – основной руководящий орган сектора стандартизации;
- Бюро по стандартизации телекоммуникаций (Telecommunication Standardization Bureau) – исполнительное подразделение сектора стандартизации;
- Исследовательские группы (всего их 14);
- Консультативная группа по стандартизации телекоммуникаций (Telecommunication Standardization Advisory Group) – вспомогательное подразделение, осуществляющее координационную работу.

Высшим органом власти Союза является Полномочная Конференция (Plenipotentiary Conference), собрание делегаций государств – членов Союза, проходящее раз в четыре года. Основные исполнительные органы — Совет и Генеральный секретариат ITU. Основные рабочие подразделения разделены на три сектора: сектор стандартизации связи, ITU-T; сектор радиосвязи, ITU-R; сектор развития электросвязи ITU-D.

ITU-R и ITU-D выполняют отдельные исследовательские, координационные и технические функции (такие как, например, регистрация радиочастот или координация работы космических телекоммуникационных спутников), тогда как Сектор стандартизации связи – ITU-T в большей степени отвечает за решение стратегических задач развития информационных технологий и инфраструктуры и, в частности, за разработку методик и стандартов, необходимых для всего мирового сообщества.

Основной целью работы ITU-T является разработка универсальных рекомендаций и международных стандартов, относящихся к различным сферам телекоммуникационных технологий и управления

Тема 3.1 – Международные организации планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

телекоммуникациями. Разрабатываемые рекомендации обеспечивают основу для развития рынка услуг связи, создания совместимых технических и организационных систем и др. С точки зрения обеспечения информационной безопасности наиболее значимыми стали рекомендации, относящиеся к серии "X – Сети передачи данных и связь открытых систем" и, в частности, к серии "X.8xx – Безопасность".

В соответствии с Резолюцией 1 Всемирной ассамблеи по стандартизации телекоммуникаций 2000-го года, была введена практика назначения Ведущих исследовательских групп (Lead Study Groups, LSGs) по определенным вопросам, требующим одновременной координации усилий нескольких исследовательских групп, которые работают в различных областях. Начиная с сентября 2001 года функционирует "Исследовательская группа 17: Сети передачи данных и телекоммуникационное программное обеспечение" ("Study Group 17: Data Networks and Telecommunication Software"), образованная на основе существовавших до этого "Исследовательской группы 7" и "Исследовательской группы 10". С момента своего образования она является Ведущей исследовательской группой по вопросам безопасности коммуникационных систем (Communication Systems Security, CSS) и, соответственно, не только работает над обеспечением безопасности технологий, напрямую относящихся к ее компетенции, но и курирует вопросы обеспечения безопасности различных коммуникационных технологий, разрабатываемых другими исследовательскими группами.

Одной из наиболее значимых разработок этой группы в сфере информационной безопасности считается Стандарт X.509, заложивший основы развития инфраструктуры публичных ключей. Наиболее актуальными проблемами, над которыми в настоящее время работает Ведущая исследовательская группа по вопросам безопасности коммуникационных систем, являются: управление безопасностью;

Тема 3.1 – Международные организации планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

безопасность мобильных систем; безопасность систем связи служб реагирования на чрезвычайные ситуации; телебиометрия.

В целом же работа этой исследовательской группы охватывает следующие основные сферы:

- безопасность управления сетями (включает в себя работу над следующими рекомендациями: М.3010 – Принципы сетей управления телекоммуникациями, М.3016 – Обзор безопасности сетей управления телекоммуникациями и некоторые другие);

- аутентификация и службы каталогов (Х.500 – Обзор концептуальных моделей и сервисов, Х.509 – Основы технологии публичных ключей и сертификатов и некоторые другие);

- управление системами (Х.733 – Функция отчета о происшествии, Х.740 – Функция проведения аудита безопасности и некоторые другие);

- основы архитектуры безопасности (Х.800 – Архитектура безопасности инфраструктуры открытых систем для приложений ITU; Х.802 – Модель безопасности нижних уровней, Х.803 – Модель безопасности верхних уровней и некоторые другие);

- факсимильная связь (Т.36 – Возможности обеспечения безопасности при использовании факсимильных аппаратов третьей группы; Т.563 – Характеристики терминалов для использования с факсимильными аппаратами четвертой группы и некоторые другие);

- телевизионные и кабельные системы (J.170 – Спецификация безопасности IP-Cablecom и некоторые другие);

- техника обеспечения безопасности (Х.841 – Объекты информационной безопасности для контроля доступа и некоторые другие);

- мультимедийные коммуникации (Н.233 – Система обеспечения конфиденциальности для аудиовизуальных сервисов, Н.234 – Управление

ключами шифрования и системой аутентификации в аудиовизуальных сервисах и др.

Помимо разработки рекомендаций и стандартов, одним из важных направлений работы ITU также стало обеспечение информационного обмена в различных формах: распространение методических материалов, касающихся обеспечения информационной безопасности, проведение семинаров и конференций. Одним из наиболее масштабных таких мероприятий является Всемирный саммит по информационному обществу (WSIS: The World Summit On The Information Society).

2.2 Институт инженеров по электронике и электротехнике

Institute of Electrical and Electronics Engineers (IEEE) – Институт инженеров по электронике и электротехнике IEEE является одной из наиболее известных профессиональных организаций, существует с 1884 года и в настоящее время насчитывает около 380000 членов из 150 стран мира. В сферу ее интересов входит множество вопросов, связанных с электротехникой, радиоэлектроникой, вычислительной техникой, информатикой, а также некоторыми разделами физики и математики. Основные направления работы этой организации: проведение специализированных профессиональных конференций; публикация специализированных изданий; поддержка образовательной деятельности; поддержка инновационных технических и методических разработок в различных сферах; разработка и распространение технических стандартов.

В состав IEEE входят 10 региональных отделений, 38 профессиональных обществ, 4 совета и 1450 студенческих отделений. Текущее управление деятельностью на верхнем уровне осуществляется Советом директоров и Исполнительным комитетом, работу которых возглавляют Президент и Исполнительный директор. Одним из основных подразделений IEEE, специализирующихся на вопросах информационной

безопасности, является Технический комитет по безопасности и защите частной информации – "IEEE Computer Society Technical Committee on Security and Privacy" (<http://www.ieee-security.org/>). В его составе функционируют три подкомитета:

- 1) Подкомитет по стандартам (Subcommittee on Standards);
- 2) Подкомитет по академической работе (Subcommittee on Academic Affairs);
- 3) Подкомитет по специализированным конференциям (Subcommittee on Security Conferences).
- 4) Основными мероприятиями, которые проводит этот комитет, являются:
- 5) Ежегодный симпозиум по безопасности и защите частной информации (IEEE CS Symposium on Security and Privacy);
- 6) Ежегодный семинар по основам информационной безопасности (Computer Security Foundations Workshop).

Также комитет ведет работу по сбору и обобщению актуальной информации о событиях в сообществе специалистов по информационной безопасности: объявления о планируемых конференциях, отчеты о прошедших конференциях и семинарах, обзоры литературы и периодики, ссылки на ресурсы в сети Интернет и др. Специальный информационный бюллетень с этой информацией – "Cipher" – рассылается подписчикам в среднем один раз в два месяца.

2.3 Ассоциация вычислительной техники

Association for Computing Machinery (ACM) – Ассоциация вычислительной техники является одной из старейших организаций, связанных с информационными технологиями – была основана в 1947 году, на заре развития компьютерной техники. Основные задачи ACM - поддержка образовательных проектов в сфере информационных технологий,

Тема 3.1 – Международные организации планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

организация научно-практических конференций, симпозиумов и семинаров, общественно-политическая работа, связанная с информационными технологиями, публикация периодических изданий и сборников научных трудов, посвященных проблемам современных информационных технологий, поддержка электронного архива таких публикаций, а также другая подобная деятельность. Основным управляющим органом этой организации является Совет АСМ, в который входит 16 человек, в том числе президент и вице-президент. Управление текущими делами Ассоциации осуществляют четыре профильных комитета. Штаб-квартира АСМ, в которой работают основные исполнительные органы, располагается в Нью-Йорке начиная с 1960 года.

Одной из основ организации работы АСМ является разделение всего сообщества членов ассоциации на так называемые группы специальных интересов (Special Interests Group – SIG) – подразделения, специализирующиеся на отдельных относительно узких проблемах развития информационных технологий. Всего АСМ объединяет 34 группы, специализирующиеся на различных вопросах разработки и использования программного обеспечения, аппаратных средств и телекоммуникаций. Каждая из групп самостоятельно определяет для себя границы своей деятельности, а их политика и финансовые вопросы координируются одним из комитетов.

Одна из этих групп – Special Interest Group on Security, Audit and Control (SIGSAC, Группа специальных интересов по вопросам безопасности, аудита и контроля, <http://www.acm.org/sigs/sigsac/>) – специализируется на вопросах информационной безопасности. Основной задачей данной группы является организация работы специализированных научно-практических конференций, таких как: симпозиум по технологиям и моделям управления доступом (SACMAT: ACM Symposium on Access Control Models and

Technologies), проводимый ежегодно начиная с 1995 года; конференция по безопасности компьютеров и коммуникаций (CCS: ACM Conference on Computer and Communications Security), проводимая ежегодно начиная с 1993 года. Кроме того, вопросы информационной безопасности прямо или косвенно затрагиваются в работе других специализированных групп Ассоциации, таких как, например, Special Interest Group on Electronic Commerce (Группа по проблемам электронной коммерции).

2.4 Консорциум Всемирной Паутины

World Wide Web Consortium (W3C) – Консорциум Всемирной Паутины.

Создание W3C было инициировано в 1989 году с целью разработки единых, согласованных стандартов обмена информацией в глобальных сетях передачи данных, а официально создание консорциума было оформлено в 1994г. Его основными задачами являются:

- обеспечение возможности доступа к сети Интернет для как можно большего числа людей вне зависимости от знания иностранных языков, культурной принадлежности, географического положения и доступных им технических средств и технической инфраструктуры;
- обеспечение возможности подключения к Интернет различных технических устройств;
- обеспечение возможности структурирования и формализации информации, доступной через Интернет, с целью сделать ее как можно более пригодной для автоматизированной обработки;
- обеспечение надежности и безопасности обмена информацией, а также возможности участвовать в информационном обмене с тем уровнем защищенности, который отдельные пользователи считают для себя подходящим.

К настоящему времени консорциум объединяет более четырехсот ведущих технологических и телекоммуникационных компаний,

правительственных организаций, исследовательских центров, институтов и университетов по всему миру. Кроме того, в штате консорциума состоят около 70 независимых технических экспертов, обеспечивающих его работу. Финансирование деятельности осуществляется за счет членских взносов, а основные административные функции и повседневная деятельность выполняются на базе трех организаций:

- 1) Массачусетский технологический институт (США).
- 2) Европейский консорциум по исследованиям в области информатики и математики (Франция).
- 3) Университет Кейо (Япония).

Помимо формирования стандартов ("рекомендаций"), эта организация также занимается образовательной деятельностью и предоставляет возможности для обсуждения различных вопросов, связанных с функционированием Интернет. Деятельность консорциума организована в виде групп: Рабочие группы (занимаются проработкой технических вопросов), Группы специальных интересов и Координационные группы (обеспечивают взаимодействие между другими группами). В каждую группу входят представители организаций-участников консорциума и приглашенные эксперты. Сферы работы консорциума ("домены", Domain), разделены на направления (Activities). Работа по двадцати четырем направлениям выполняется в общей сложности шестьюдесятью группами.

Вопросами информационной безопасности занимается сфера "Технология и общество" (Technology and Society Domain) в рамках специального направления "Безопасность" (W3C Security Activity), состоящего из двух рабочих групп. Также до 2006 года в составе Консорциума функционировало направление "Защита частной информации" (Privacy).

Тема 3.1 – Международные организации планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

К работам консорциума в сфере информационной безопасности относятся: разработка стандарта цифровых подписей для информационных ресурсов (PICS Signed Labels 1.0 Specification); разработка системы электронной подписи для документов XML; разработка стандартов передачи зашифрованных данных с использованием языка XML.

2.5 Международная организация по стандартизации

International Organization for Standardization (ISO) – Международная организация по стандартизации. ISO в нынешнем виде была учреждена в 1946г. и представляет собой неправительственное объединение национальных организаций по стандартизации, нацеленное на унификацию стандартов (главным образом, технических) в различных областях производственной деятельности и оказания услуг.

Помимо основных членов (156 стран), непосредственно участвующих в работе, в ISO также входят члены-корреспонденты (Correspondent member) – страны, не имеющие полноценных органов стандартизации, а также члены-подписчики (Subscriber member) – страны с небольшими экономиками, получающие необходимую справочную информацию на льготных условиях.

Главным органом управления ИСО является ежегодная Генеральная Ассамблея, принимающая стратегические решения, касающиеся развития всей организации. Подготовкой материалов для принятия таких решений занимается Совет ИСО, собрания которого проходят два раза в год. Непосредственно разработкой стандартов занимаются технические комитеты и подкомитеты, в работе которых принимают участие представители заинтересованных стран. За разработку каждого документа в подкомитете отвечает специально создаваемая для этого рабочая группа. Проекты международных стандартов, принятые техническими комитетами, рассылаются в национальные организации для голосования; документ

Тема 3.1 – Международные организации планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

приобретает статус международного стандарта, если за него проголосовало не менее 75% членов, участвовавших в голосовании.

Основным подразделением ИСО, занимающимся вопросами информационной безопасности, является Объединенный технический комитет JTC 1 "Информационные технологии", в состав которого входит подкомитет SC 27 "Средства безопасности в информационных технологиях" (IT Security techniques). За время своей работы этот подкомитет разработал более 60 международных стандартов, относящихся к информационной безопасности.

С вопросами информационной безопасности также связана работа подкомитета SC 37 "Биометрическая идентификация" (Biometrics) и подкомитета SC 17 "Карточки и персональная идентификация" (Cards and personal identification).

1 Специализированные международные организации в сфере планирования и управления информационной безопасностью

1.1 Характеристика специализированных международных организаций в сфере управления информационной безопасностью

Специализированные организации, имеющие глобальное влияние на управление информационной безопасностью на различных уровнях и общее состояние информационной безопасности, как правило, могут функционировать на базе:

- частных компаний, занимающихся исследованиями, разработками и консультированием в сфере информационной безопасности;
- крупных учебных заведений, специализирующихся на информационных технологиях, а также обладающих существенным авторитетом и финансовыми ресурсами;
- правительственных учреждений, ответственных за обеспечение информационной безопасности в определенных сферах.

Основным направлением организационной работы, осуществляемой в такой форме, становится формирование и поддержание баз данных, содержащих информацию о ставших известными уязвимостях различных программных и аппаратных средств, а также другие формы и направления информационной, консультативной и методической работы в данной сфере. Важными факторами успешности функционирования таких организаций является объединение информации из как можно большего числа источников (в частности, от как можно большего числа специалистов и компаний, занимающихся проблемами информационной безопасности) и как можно более эффективное распространение сведений (знаний) в сообществе пользователей информационных систем.

Ввиду того, что такая форма организационной работы основана на частных компаниях и относительно небольших учреждениях, подходы к

организации и управлению обычно не подчиняются каким-либо общим правилам. Также состав таких организаций может со временем меняться: на смену одним исследовательским центрам могут приходить другие – более успешные и эффективные – с теми же функциями. В настоящее время можно выделить следующие наиболее значимые организации, занимающие эту нишу: CERT Coordination Center – Координационный центр CERT; исследовательская группа X-Force компании IBM.

1.2 Координационный центр CERT CERTCC

CERT Coordination Center (CERT/CC) – Координационный центр CERT CERTCC, возникшая в 1988 году как Computer security incident response team (Группа реагирования на инциденты, связанные с компьютерной безопасностью), функционирует на базе Института разработки программного обеспечения при Университете Карнеги-Мелон (Software Engineering Institute, Carnegie Mellon University) и финансируется Министерством обороны и Министерством национальной безопасности США. Наряду с проведением независимых исследований и решением различных задач по обеспечению безопасности глобальной информационной инфраструктуры, эта организация обеспечивает централизованный сбор сведений обо всех уязвимостях в различных информационных системах и поддержание актуальной базы знаний об уязвимостях в информационных системах. Сведения о вновь выявляемых уязвимостях, вредоносных программах и способах нарушения информационной безопасности рассылаются по электронной почте: подписчиками этого бюллетеня являются более 161000 специалистов во всем мире. В рамках этой деятельности CERT/CC осуществляет постоянную исследовательскую работу:

- определение характера возможных последствий использования выявленных уязвимостей и вирусов;
- анализ имеющихся средств использования уязвимостей;

Тема 3.2 – Специализированные международные организации и объединения планирования и управления информационной безопасностью
(Управление информационной безопасностью)

- анализ того, насколько активно используются уязвимости и насколько широко распространены вирусы;
- взаимодействие с поставщиками информационных систем с целью более глубокого анализа выявляемых уязвимостей.

На основе проводимого анализа CERT/CC разрабатывает меры по устранению уязвимостей и рекомендации по уменьшению негативных последствий. По результатам этой работы всем подписчикам рассылается информация об угрозах информационной безопасности и возможных способах их устранения. Также на основе этих данных формируется специальная справочная и техническая документация, проводится дальнейшая исследовательская и методическая работа. В частности, CERT/CC поддерживает программу безопасной разработки ПО ("secure coding"), основывающуюся на том, что большая часть уязвимостей возникает в следствие относительно небольшого числа ошибок в программном коде информационных систем. Таким образом, CERT/CC на основе накопленных результатов анализа уязвимостей ведет целенаправленную работу по выявлению типичных программных ошибок, выработке стандартов безопасного программирования и распространению этой информации среди разработчиков ПО. Помимо основной информационной работы с уязвимостями CERT также занимается сопутствующими видами деятельности:

- организация учебных курсов по различным направлениям (сетевая безопасность, управление информационными рисками, организация работы групп реагирования);
- сертификация специалистов по реагированию на инциденты в сфере информационной безопасности;
- поддержка фундаментальных научных исследований в различных областях информационной безопасности, таких как методы разработки

безопасных приложений, выявление уязвимостей, анализ шпионского ПО, решение вопросов безопасности как составная часть процесса разработки и др.;

- содействие развитию локальных (национальных и корпоративных) групп реагирования на инциденты.

1.3 Исследовательская группа X-Force

X-Force security intelligence team – Исследовательская группа X-Force. Деятельность этой группы является одним из направлений бизнеса компании Internet Security Systems (ISS) – наиболее авторитетного поставщика комплексных решений в сфере информационной безопасности, клиентами которого являются все без исключения крупнейшие компании США, а также правительственные организации. В конце 2006 года ISS была куплена компанией IBM и интегрирована в нее в качестве самостоятельного подразделения. Одной из задач группы X-Force является поддержание в актуальном состоянии базы данных известных уязвимостей различных программных и аппаратных платформ. База данных, поддерживаемая этой группой, доступна по сети Интернет и постоянно пополняется сведениями о новых уязвимостях (в настоящее время их насчитывается более 40000). Основные причины, по которым данная организация является ведущей в этой области, следующие:

- большое количество крупных компаний-клиентов, от которых постоянно поступает информация о нападениях, уязвимостях и др.;
- наличие собственной научно-исследовательской базы, на основе которой постоянно осуществляется выявление новых уязвимостей и обобщение сведений об уязвимостях, полученных из различных источников;
- использование специально разработанных универсальных классификаций (в частности, общего словаря наименований уязвимостей –

Common Vulnerabilities and Exposures, CVE) для хранения и обработки информации в базах данных известных уязвимостей.

Также одним из направлений справочно-информационной деятельности этой исследовательской группы является оказание услуг по индивидуальному анализу угроз и информированию (X-Force Threat Analysis Service (XFTAS)). Данный комплекс услуг позволяет заказчикам ежедневно получать адаптированную актуальную информацию об угрозах и уязвимостях с учетом особенностей построения их информационных систем (платформ, приложений, сферы ведения бизнеса, географического положения) и включает в себя: информацию об угрозах; экспертный анализ угроз; описание текущего и прогнозного состояния угроз; рекомендуемые способы устранения угроз; количественный анализ атак за последние 30 дней. Еще одной из задач группы является выпуск периодических (ежеквартальных, ежегодных) информационных бюллетеней с обзорами наиболее значимых событий в сфере информационной безопасности.

2 Специализированные международные объединения в сфере управления информационной безопасностью

2.1 Характеристика специализированных международных объединений в сфере управления информационной безопасностью

Альянсы крупных технологических компаний. Совместные альянсы (ассоциации, коалиции, группы) крупных (иногда средних) технологических и консультационно-исследовательских компаний представляют собой временные (заключаемые на краткосрочную или среднесрочную перспективу) или долгосрочные соглашения между несколькими фирмами, направленные на совместное, скоординированное, целенаправленное решение определенных масштабных и ресурсоемких задач развития технологии, формирования рыночного спроса на определенные продукты и организации инфраструктуры информационной безопасности. Высокая

Тема 3.2 – Специализированные международные организации и объединения планирования и управления информационной безопасностью
(Управление информационной безопасностью)

значимость такой формы организационной работы в сфере информационной безопасности, как формирование альянсов крупными и средними компаниями, специализирующимися на информационных технологиях, обусловлена тем, что:

- такие альянсы способны осуществить наиболее крупные инвестиции в разработку новых технологий и проведение исследований, которые могут повлиять на все развитие информационных технологий и состояние дел в сфере информационной безопасности;

- компании, входящие в такие альянсы, занимают значительную долю рынка и потому определяют общее направление развития информационных технологий вообще и средств защиты информации в частности;

- такие альянсы компаний способны создать комплексные технологии, продукты и решения, охватывающие различные аспекты функционирования информационных систем и средств защиты информации, и таким образом достичь нового уровня защищенности информации, что практически невозможно при работе компаний (даже самых крупных) по отдельности.

Как правило, каждый такой альянс является уникальным, и участники в каждом конкретном случае определяют условия работы в рамках такой организационной формы. На конкретный подход к организации альянса могут повлиять такие факторы, как:

- характер целей и задач, которые ставятся перед альянсом;
- текущее состояние дел в той области, для работы в которой создается альянс;
- состав участников альянса, их роль и место на рынке информационных технологий;

Тема 3.2 – Специализированные международные организации и объединения планирования и управления информационной безопасностью
(Управление информационной безопасностью)

- наличие возможных конкурентов (например, аналогичных альянсов параллельно создаваемых другими группами компаний);
- ранее сложившиеся взаимоотношения между компаниями – участниками альянса и др.

Задачами формирования альянсов могут быть:

- разработка новых продуктов и услуг, а также базовых технологий, протоколов, алгоритмов и соглашений, на основе которых такие продукты и услуги в будущем могли бы разрабатываться;
- формирование новых рынков сбыта и поддержка существующих;
- влияние на государственные и общественные организации, а также на сообщество пользователей информационных систем с целью обеспечения развития и более широкого использования информационных технологий и средств информационной безопасности;
- влияние на систему профессиональной подготовки специалистов с целью обеспечения качества их обучения.

Основными типичными приемами организационной работы на таком уровне являются:

- скоординированный выбор и унификация технических решений (аппаратных устройств, программных алгоритмов), используемых в системах передачи и обработки информации и/или системах защиты информации;
- информационная поддержка как производителей информационных систем и поставщиков решений (входящих в альянс и не входящих в него), так и потребителей и пользователей (потенциальных и настоящих);
- скоординированное разделение функций по разработке отдельных элементов информационной технологии в рамках общей согласованной стратегии развития;
- скоординированная маркетинговая и информационная политика, направленная на обеспечение использования (поддержки, совместимости)

создаваемых решений (технологий, протоколов и др.) как можно большим числом потребителей и независимых производителей, а также ее признание правительственными структурами;

– совместное влияние на органы государственной власти (лоббирование) с целью обеспечения государственной поддержки определенных продуктов, проектов, технологий и архитектур информационных систем и систем защиты информации.

2.2 Альянс по смарт-картам – SCA

Smart Card Alliance (SCA) – Альянс по смарт-картам. SCA (<http://www.smartcardalliance.org>) занимается вопросами развития технологии смарт-карт – одной из ключевых технологий в сфере информационной безопасности, используемой для идентификации пользователей различных сервисов и информационных систем (таких как мобильные телефонные сети, банковские "электронные кошельки" и др.). Этот долгосрочный (стратегический) альянс был образован в начале 2001 года путем слияния двух организаций: Smart Card Industry Association и Smart Card Forum. В состав альянса входят около сотни различных компаний и правительственных организаций. При этом в составе участников альянса выделяются несколько групп:

1) Руководящий Совет (Leadership Council) – ведущие компании, определяющие основную политику Альянса: Visa USA, Bank of America, IBM, Lockheed Martin, Intel, Mastercard International и некоторые другие (всего более двадцати компаний).

2) Основная группа членов Альянса – различные фирмы, так или иначе связанные с вопросами информационной безопасности, поставкой соответствующих продуктов и услуг (такие как Texas Instruments Incorporated, Sun Microsystems и другие) – всего около 70 компаний.

3) Члены – правительственные организации. В эту группу входят как федеральные правительственные учреждения США (Государственный департамент, Министерство национальной безопасности и другие), так и местные органы власти (Портовая администрация Нью-Йорка, Транспортная администрация Вашингтона и другие) – всего около 30 членов.

Также в состав Альянса входит один университет и несколько ассоциированных членов. Работу альянса возглавляют Совет директоров во главе с председателем и Исполнительный директор. Деятельность альянса разделена на членские советы (Member Council) по отдельным сферам интересов:

- 1) Совет по бесконтактным и мобильным платежам.
- 2) Совет по здравоохранению (специализируется на вопросах использования смарт-карт в сфере здравоохранения).
- 3) Совет по идентификации.
- 4) Совет по системам контроля за физическим допуском.
- 5) Совет по транспорту (специализируется на вопросах продвижения и адаптации смарт-карт в транспортной сфере).

Каждый совет управляется председателем, вице-председателями и управляющим комитетом. Направления работы Альянса включают в себя:

- организацию специализированных ежегодных конференций;
- организацию образовательных программ и системы сертификации специалистов;
- издание различных информационных и справочных материалов как технического, так и управленческого характера;
- ведение централизованной базы данных поставщиков оборудования и услуг в сфере смарт-карт.

Internet Security Alliance (ISA) – Альянс по безопасности сети Интернет. ISA был создан в апреле 2001 года по инициативе двух крупных

авторитетных организаций: CERT/CC Университета Карнеги-Меллон и Ассоциации электронной промышленности (Electronic Industries Alliance, EIA). Уже к середине 2004 года в альянс входило около тридцати членов, в числе которых такие крупные компании, как Boeing, NEC, Mitsubishi, Federal Express, AIG, Sony, Symantec и другие. Работой Альянса руководит Совет директоров, в который входят авторитетные представители наиболее известных компаний-членов. Кроме того, в состав альянса входят около тридцати ассоциированных членов. На первоначальном этапе создания альянса его основной задачей было повышение эффективности обмена информацией об уязвимостях, распространяемой CERT/CC. В дальнейшем круг задач альянса расширился, и теперь работа ведется по следующим направлениям:

- создание эффективных механизмов обмена информацией об уязвимостях в сети Интернет и найденных решениях проблем безопасности;
- исследование фундаментальных проблем безопасности;
- развитие программ профессиональной подготовки и сертификации специалистов по информационной безопасности;
- взаимодействие и государственными органами законодательной и исполнительной власти.

2.3 Международная ассоциация компаний-производителей биометрического оборудования

The International Biometric Industry Association (IBIA) – Международная ассоциация компаний-производителей биометрического оборудования. Ассоциация была создана в 1998 году с целью коллективной поддержки интересов компаний, связанных с производством биометрического оборудования. Основной задачей альянса является взаимодействие с потенциальными заказчиками их продукции (как среди коммерческих компаний, так и в общественном секторе) с целью продвижения средств

биометрической идентификации. Членами ассоциации являются около 30 компаний и организаций, среди которых Hitachi, LG Electronics, Panasonic, NEC и другие. Управление текущими делами осуществляет Совет директоров в составе одиннадцати человек, а также исполнительный директор. Деятельность Ассоциации разделена на шесть рабочих групп, среди которых:

- рабочая группа по стандартам и технологиям. Ее основная цель – защищать базовые интересы членов альянса в сфере стандартизации биометрических технологий и систем, использующих биометрию;
- рабочая группа по потребительским приложениям. Занимается ориентацией рынка потребительских систем на более широкое использование биометрических технологий;
- рабочая группа по международным рынкам. Осуществляет контакты с другими биометрическими организациями по всему миру;
- рабочая группа по образованию, маркетингу и информированию. Обеспечивает информационное присутствие компаний-членов ассоциации в различных областях через реализацию маркетинговых мероприятий и образовательных программ;
- рабочая группа по глобальной политике. Проводит информационную работу с представителями правительственных структур по всему миру.

1 Методология управления информационной безопасностью поставщиками информационных систем

В последнее десятилетие – период, когда произошло широкое распространение автоматизированных информационных систем, их объединение в единую глобальную сеть и массовое использование миллионами пользователей одних и тех же компонентов информационных систем (операционных систем, аппаратных платформ, протоколов обмена информацией), – большое значение приобрело то, как поставщики подобных универсальных платформ и компонентов (являющиеся иногда практически монополистами на определенных сегментах рынка) организуют работу по повышению уровня информационной безопасности по различным направлениям. Уровень влияния таких компаний на состояние дел в сфере информационной безопасности иногда может быть очень значительным – даже большим, чем международных организаций и некоторых правительственных структур.

Основные задачи организационной работы крупных (т.е. занимающих большую долю рынка) поставщиков широко используемых информационных систем в сфере информационной безопасности:

- закрепить свои рыночные позиции путем создания благоприятного имиджа в глазах покупателей и всего сообщества пользователей информационных систем;
- занять новые рыночные ниши, предъявляющие более строгие требования к уровню информационной безопасности по сравнению с массовым рынком (банковский сектор, правительственные структуры и др.);
- обеспечить эффективную интеграцию поставляемых продуктов в различные информационные системы и бизнес-процессы;
- избежать обвинений (в том числе и судебных исков) со стороны потребителей, чьи информационные системы могли бы подвергнуться атакам.

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

Приемы и методы управления информационной безопасностью на этом уровне в каждом случае могут быть различными и определяются для каждой компании-поставщика следующими основными факторами:

- характером продуктов, поставляемых на рынок;
- состоянием (конъюнктурой) рынка информационно-технологических продуктов такого типа и поведением конкурентов;
- политикой государственных структур как в отношении вопросов информационной безопасности вообще, так и в отношении отдельных компаний-поставщиков информационных систем, в частности;
- задачами, целями и основными способами использования поставляемых продуктов пользователями;
- общим состоянием дел в сфере информационной безопасности, информационной культурой, развитием и распространением преступности;
- формируемым общественным мнением в отношении вопросов информационной безопасности и отдельных компаний-поставщиков.

Организационная работа в сфере информационной безопасности на уровне таких компаний разделяется на два основных под-направления:

- организация работы внутри компаний, специально направленной на обеспечение информационной безопасности выпускаемых продуктов;
- организация внешнего взаимодействия с потребителями, партнерами, государственными структурами и другими участниками.

Внутренняя организационная работа по обеспечению информационной безопасности производимых и продаваемых продуктов является неотъемлемой частью процесса проектирования, производства и маркетинговой поддержки этих продуктов. Однако при этом выделяются дополнительные специальные мероприятия, осуществляемые отдельно от основных производственно-сбытовых процессов в компаниях – крупных производителях информационных систем. Примерами таких специальных

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем

(Планирование и управление информационной безопасностью)

организационных мероприятий является создание специальных подразделений, чьей основной задачей является контроль за устранением существующих уязвимостей и выполнение сопутствующих функций, а также обучение разработчиков специальным методам разработки программного обеспечения и аппаратных средств, не содержащих уязвимостей.

Основные приемы и методы внешней организационной работы в сфере информационной безопасности на уровне крупных компаний–поставщиков информационных систем могут быть следующие:

- организация информационного обмена с пользователями выпускаемых продуктов – программных и аппаратных средств (информирование о выявленных уязвимостях и способах их устранения, получение информации об уязвимостях, выявленных пользователями, а также других возникающих проблемах);

- организация деятельности в сфере подготовки специалистов (система подготовки квалифицированного инженерно-технического персонала, специализирующегося на определенных программных продуктах и, в частности, на администрировании средств защиты информации, сетевых операционных систем и т.п.);

- организация профессиональных конференций, которые способствуют обмену опытом и информацией, связанной с повышением уровня информационной безопасности при использовании определенных программных и аппаратных платформ;

- организация взаимодействия с правительственными организациями (в том числе по вопросам сертификации программных и аппаратных средств на соответствие требованиям национальных стандартов и правил);

- создание и поддержание системы сертификации специалистов, ориентированной на определенные программные продукты и аппаратные системы (в том числе, организация взаимодействия со специализированными

компаниями, занимающимися профессиональным тестированием специалистов и др.).

Организация информационного обмена с пользователями продуктов является одним из наиболее важных направлений деятельности компаний в данной сфере. Эта работа включает в себя сбор информации, ее анализ, а также принятие решений о том, необходимо ли информировать все сообщество пользователей, которых может коснуться выявленная уязвимость, или только ограниченный круг доверенных специалистов, имеющих необходимые полномочия и авторитет. Дальнейшие действия, как правило, связаны с уведомлением пользователей о возможных способах решения проблем (потенциальных или уже возникших) и информированием о возможных последствиях реализации угроз.

2 Управление информационной безопасностью поставщиками информационных систем

2.1 Корпорация Microsoft

Корпорация Microsoft является крупнейшим в мире производителем программного обеспечения – ее программные продукты распространены по всему миру. В частности, Microsoft производит и поставляет следующие основные программные средства:

- операционные системы для рабочих станций (пользовательских персональных компьютеров) семейства Windows;
- операционные системы для сетевых серверов (веб-серверов, серверов баз данных, файл-серверов и др.) – старшие версии операционных систем семейства Windows;
- операционные системы для мини-компьютеров (PDA) – семейства Windows CE и Windows Pocket PC;
- специализированные функциональные серверы: серверы реляционных баз данных (Microsoft SQL Server), веб-серверы (IIS – Internet

Information Server), системы построения хранилищ данных (Analysis Services) и некоторых других;

- средства разработки приложений;
- пользовательские программные продукты для платформы Windows: веб-браузеры, почтовые клиенты, программы верстки в формате HTML, офисные приложения, мультимедийные приложения и другие.

Также корпорацией Microsoft была приобретена компания, занимающаяся поставками систем управления предприятиями (систем класса ERP – Enterprise Resource Planning).

В силу того, что программными продуктами Microsoft пользуется большинство пользователей персональных компьютеров (как частных, так и в коммерческих и правительственных организациях), а на основе серверных программных платформ Microsoft функционирует большинство информационных систем, обеспечивающих обработку, хранение и передачу информации (в том числе и в сети Интернет), организационная работа этой корпорации в сфере информационной безопасности имеет глобальное значение.

Внутренняя организационная работа в сфере информационной безопасности продуктов корпорации Microsoft включает в себя:

- проведение специальных тренингов и дополнительного обучения разработчиков программного обеспечения специальным методам, обеспечивающим надежность и безопасность производимого программного обеспечения (включая внедрение и использование для разработки собственных продуктов методологии Жизненного цикла безопасной разработки);
- организацию специального Центра решения вопросов безопасности (Microsoft Security Response Center, MSRC), основными задачами которого являются постоянный сбор информации и поиск новых уязвимостей, принятие

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

мер к устранению выявленных уязвимостей, координация работы разработчиков и недопущение появления ранее выявленных уязвимостей в новых продуктах в будущем.

В организационной структуре Microsoft помимо MSRC существуют еще одно подразделение, специализирующееся на решении вопросов безопасности – Центр защиты от вредоносных программ (Microsoft Malware Protection Center, ММРС). Он включает в себя несколько лабораторий, расположенных по всему миру, и занимается исследованием вредоносных программ, обеспечивает методическую поддержку разработки различных средств защиты (таких, как Windows Live OneCare, Windows Defender, Malicious Software Removal Tool), а также участвует в процедурах реагирования на возникновение новых угроз безопасности.

Основными направлениями внешней организационной работы корпорации Microsoft в сфере информационной безопасности являются:

- систематическое информирование пользователей операционных систем Windows (а также других программных продуктов) о выявленных уязвимостях и распространение информации о том, как эти уязвимости могут быть ими устранены;
- реализация программы упреждающих защитных действий – Microsoft Active Protections Program (MAPP);
- поддержка обучения пользователей программных продуктов (в основном администраторов серверных платформ);
- разработка и поддержка методологии Жизненного цикла безопасной разработки – Microsoft Security Development Lifecycle (SDL);
- партнерская программа Microsoft Security Partners – Партнеры Microsoft в сфере безопасности;
- Government Security Program (GSP) – Программа обеспечения безопасности правительств;

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

- организация конференций по различным аспектам использования программных продуктов Microsoft;
- организация специального фонда для борьбы с хакерами;
- организация централизованной сертификации своих продуктов в государственных органах;
- проведение собственной конференции по безопасности.

1) Организация информирования пользователей о выявленных уязвимостях – строится на основе т.н. Бюллетеней Безопасности ("Security Bulletin"), выпускаемых с определенной периодичностью, а также по мере выхода специальных обновлений, устраняющих выявленные уязвимости (т.н. "заплат", patches). Порядок выпуска этих бюллетеней, их содержание и другие вопросы регулируются специальным организационным документом – Процедурой Выпуска Бюллетеней Безопасности (Security Bulletin Release Process). Также в рамках этой работы организован сбор информации об уязвимостях, выявляемых пользователями: на Интернет-сайте компании размещена специальная форма, заполнив которую, каждый желающий может сообщить о новых самостоятельно обнаруженных уязвимостях в программных продуктах.

2) Программа упреждающих защитных действий – Microsoft Active Protections Program (MAPP) – представляет собой систему ускоренного информирования разработчиков систем безопасности (антивирусов, систем обнаружения и предотвращения вторжений) о вновь выявленных уязвимостях. Данная программа реализуется для того, чтобы сторонние разработчики систем безопасности могли не дожидаться выхода очередного Бюллетеня Безопасности и как можно раньше начать разрабатывать механизмы нейтрализации новых уязвимостей на основе своих программных решений. Для участия в данной программе допускаются разработчики систем защиты на

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

основе программных платформ Microsoft, клиентская база которых составляет не менее 10000 пользователей.

3) Поддержка системы обучения пользователей и администраторов реализуется несколькими основными способами:

- целенаправленная подготовка и опубликование учебных пособий, справочников, статей и других учебных материалов, содержащих пояснения, пошаговые инструкции, примеры конфигурации и сценарии для установки программных продуктов, в том числе и такие, которые должны обеспечить решение вопросов информационной безопасности;

- организация и методическая поддержка системы профессионального обучения и сертификации специалистов по различным программным продуктам (в том числе администраторов сетевых операционных систем, баз данных и других серверных продуктов, таких как Internet Security and Acceleration Server). Такая поддержка включает в себя сертификацию преподавателей учебных центров, сертификацию самих учебных центров, а также установление партнерских отношений с организациями, занимающимися профессиональным обучением и профессиональным тестированием администраторов и разработчиков информационных систем;

- проведение бесплатных семинаров для администраторов операционных систем, посвященных вопросам обеспечения информационной безопасности (в частности, функциональным возможностям тех или иных программных продуктов, обеспечивающим решение определенных вопросов защиты информации).

4) Одним из направлений информационной и методической поддержки сообщества специалистов является продвижение и популяризация среди разработчиков информационных систем методологии Жизненного цикла безопасной разработки – Microsoft Security Development Lifecycle (SDL). Данная методология представляет собой набор универсальных методических,

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

технических и организационных рекомендаций и приемов, в совокупности обеспечивающих существенное повышение уровня безопасности разрабатываемого ПО. Так, по утверждению Microsoft, после внедрения данной методологии ей удалось снизить общее число уязвимостей, выявленных в SQL Server в течение трех лет после выпуска продукта на рынок, на 91% (если в MS SQL 2000 было выявлено 34 уязвимости, то в MS SQL 2005 – всего 3 уязвимости).

Продвижение данной методологии в среде разработчиков информационных систем включает в себя:

- опубликование и постоянное развитие самой методологии;
- организацию профессионального сообщества (SDL Pro Network), которое объединяет консалтинговые компании и учебные центры, специализирующиеся на вопросах безопасности;
- разработку и распространение шаблонов для среды разработки Visual Studio, поддерживающих выполнение положений методологии.

5) Microsoft Security Partners – программа построения партнерских отношений с различными независимыми компаниями, работающими в сфере информационной безопасности. Данная программа развивается по нескольким самостоятельным направлениям:

- Antivirus Partners – Партнерство в создании антивирусных и защитных программ, а также в обмене актуальной информацией о новых вирусах, воздействующих на различные продукты Microsoft. В этой программе участвуют такие фирмы, как Symantec, ДиалогНаука, Лаборатория Касперского, Panda Software и другие (всего около 20 различных компаний);
- Альянс SecureIT – партнерство с разработчиками решений в сфере безопасности (VeriSign, Trend Micro, Symantec и др.) по совместной разработке новых средств в данной области. Члены альянса получают от Microsoft и друг

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками
информационных систем
(Планирование и управление информационной безопасностью)

от друга закрытую информацию о новых разработках, позволяющую создавать интегрируемые и взаимодействующие решения;

- ISA Server Partners – партнерство с разработчиками программных и аппаратных решений, адаптированных для платформы Internet Security and Acceleration Server;

- Microsoft Windows Rights Management Services Partners – Партнерство с компаниями-разработчиками программных продуктов, разработчиками аппаратных средств идентификации и системными интеграторами в вопросах более полного использования функциональных возможностей ОС Windows, связанных с управлением правами пользователей и доступом к информационным ресурсам. Данная программа включает в себя три категории партнеров: Независимых поставщиков ПО, Разработчиков инфраструктурных решений и Системных интеграторов.

6) Government Security Program (GSP) – Программа обеспечения безопасности правительств – представляет собой инициативу по передаче правительственным структурам различных стран исходных кодов программных продуктов (главным образом, операционных систем) для того, чтобы у специалистов и экспертов была возможность убедиться в отсутствии существенных изъянов в этом программном обеспечении. Такой анализ должен дать основания для признания этих программных продуктов надежными с точки зрения информационной безопасности и, таким образом, расширить возможности их применения различными организациями (как правительственными, так и частными). Также предполагается, что эта программа должна помочь устранить имеющиеся недоработки в программном обеспечении и расширить партнерство между Microsoft и правительствами различных стран в сфере защиты информации. В рамках программы участвующим в ней экспертам также предоставляется доступ к документации, справочные материалы, специальные средства для работы с исходными

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

кодами и поддержка со стороны специалистов Microsoft. В данную программу включены около 60 стран (в том числе и Россия в лице ФСТЭК), отвечающих определенным требованиям к защите прав на интеллектуальную собственность.

Одной из возможных причин начала реализации этой программы явилось то, что некоторые правительства (например, Германии) заявили о возможном переходе правительственных и муниципальных учреждений на альтернативные операционные системы (такие как, например, Linux), для которых доступны исходные коды. Развитие этой тенденции в перспективе могло привести (и отчасти уже привело) к определенной потере рынков сбыта продукции Microsoft.

7) Централизованная сертификация программных продуктов в государственных органах является для корпорации Microsoft одним из направлений реализации концепции развития защищенных информационных систем и предполагает возможность использования программного обеспечения этой компании в информационных системах, к которым предъявляются особые требования с точки зрения надежности и информационной безопасности. Так, сертификация ФСТЭК операционных систем и систем управления базами данных, поставляемых Microsoft, позволила использовать эти программные продукты в автоматизированных системах учета и контроля ядерных материалов на предприятиях Минатома РФ и в других организациях. Первый проект по сертификации продуктов Microsoft в России был начат в 1996 году и продолжался на протяжении примерно трех лет с участием не только специалистов Гостехкомиссии РФ и Microsoft, но и представителей Минатома РФ и Министерства энергетики США. Также Microsoft ведет работу по сертификации некоторых своих продуктов на соответствие стандарту Common Criteria for Information Technology Security Evaluation – универсальному стандарту обеспечения

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками
информационных систем

(Планирование и управление информационной безопасностью)

информационной безопасности, официально признаваемому многими государствами.

Конференция по безопасности BlueHat проводится с 2005 года дважды в год для обмена мнениями и идеями по различным вопросам информационной безопасности. В ней участвуют только специалисты, приглашаемые компанией Microsoft.

2 Корпорация Cisco Systems

Компания Cisco Systems, основанная в 1984 году группой специалистов Стэнфордского университета, в настоящее время является мировым лидером в производстве оборудования для сетей передачи данных. На основе оборудования, произведенного этой компанией, функционируют глобальные сети передачи данных, а также сети многих правительственных организаций и крупных компаний.

В связи с тем, что оборудование этой компании обеспечивает функционирование большинства наиболее значимых и ответственных сетей передачи данных, ее организационная поддержка решения вопросов информационной безопасности имеет глобальное значение.

В число основных направлений организационной работы компании Cisco входят:

- поддержка сети образовательных центров – Сетевая Академия Cisco – при различных учебных учреждениях и предприятиях. Работа Сетевых Академий по всему миру обеспечивает подготовку специалистов по администрированию сетей и обеспечению сетевой безопасности и централизовано поддерживается головным офисом, который осуществляет подготовку преподавателей, предоставляет учебные материалы, ведет учет слушателей, осуществляет экзаменационное тестирование выпускников, выписывает международные сертификаты и т.д. В России функционирует более 50-ти Сетевых Академий Cisco;

- организация и координация работы поставщиков различных компонентов информационной инфраструктуры на основе программы Network Admission Control (NAC) – Управление Доступом в Сеть. В рамках данной программы, инициированной в 2020 году совместно с ведущими поставщиками антивирусов (Network Associates, Symantec и Trend Micro) и нацеленной на решение различных проблем информационной безопасности,

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками
информационных систем
(Планирование и управление информационной безопасностью)

Cisco планирует реализовать новые технические решения и подходы к обеспечению информационной безопасности, основанные на собственном сетевом оборудовании. В частности, кооперация с поставщиками программных продуктов в рамках данной программы должна позволить автоматически управлять подключением компьютеров, не отвечающих определенным требованиям (политикам) информационной безопасности;

- организация работы Cisco Product Security Incident Response Team (PSIRT) – Группы реагирования на инциденты, связанные с безопасностью продуктов Cisco. Основной задачей этого подразделения является сбор информации о выявленных уязвимостях, их анализ, а также координация работ по их устранению и предотвращению негативных последствий;

- распространение информации о выявленных уязвимостях и проблемах с безопасностью.

1 Общая политика США в сфере планирования и управления информационной безопасностью

В силу того, что США обладают значительным финансовым, технологическим, научно-техническим и военным потенциалом, а также уделяют большое значение усилению национальной безопасности, защите гражданских прав и интересов бизнеса, опыт этой страны в сфере управления информационной безопасностью является наиболее важным для изучения. Значимость управления информационной безопасностью в США на государственном уровне определяется также тем, что в этой стране сконцентрированы крупнейшие финансовые компании, исследовательские учреждения и корпорации, существенно влияющие на развитие технологий, финансовую стабильность и экономическое развитие всего мирового сообщества.

Одним из ключевых направлений развития информационной безопасности, так же как и во многих других странах, является обеспечение национальной (государственной) безопасности и, в частности, безопасности информационных систем т.н. «силовых» ведомств: вооруженных сил, внешней разведки и пр. Начиная примерно с 1992 года основные усилия по организации мероприятий в сфере информационной безопасности предпринимались Министерством обороны США в рамках концепции «Информационного противоборства», ориентированной на решение задач борьбы с системами управления вооруженными силами противника на различных уровнях и обеспечение безопасности и эффективности собственных информационных систем армии США. Дальнейшее развитие эта концепция получила в 1996 году в виде нового полевого устава армии США «Информационные операции».

В целом же началом современной целенаправленной систематической организационной деятельности в сфере информационной безопасности на

национальном уровне можно считать издание директивы администрации Президента Билла Клинтона Presidential Decision Directive 63 (PDD 63) «Защита критически важной инфраструктуры» от 22 мая 1998 года. На этом документе базируется подписанный Биллом Клинтон в начале 2000 года «Общенациональный план защиты информационных систем», который определяет основные направления деятельности государства и всего общества в сфере обеспечения информационной безопасности.

Также в феврале 2003 года администрацией президента Джорджа Буша-младшего была опубликована «Национальная стратегия достижения безопасности в киберпространстве» («National Strategy to Secure Cyberspace»), описывающая пять приоритетов в деятельности США по обеспечению информационной безопасности и основные задачи в рамках этих приоритетов на среднесрочную и долгосрочную перспективу.

Фактически данные документы могут считаться официальной общенациональной политикой США в сфере информационной безопасности, на основе которой строится вся система деятельности государственной власти в этой области и структура государственных органов, обеспечивающих информационную безопасность в стране.

В соответствии со стратегией информационной безопасности основными государственными приоритетами в этой области являются:

- становление и развитие национальной системы реагирования на происшествия в сфере информационной безопасности;
- реализация комплексной системы мер по уменьшению угроз информационной безопасности;
- обеспечение подготовки специалистов в сфере компьютерной безопасности и обеспечение ответственного отношения всего населения страны к вопросам защиты информации;

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США

(Планирование и управление информационной безопасностью)

- обеспечение защиты информационных систем, имеющих отношение к государственным органам;
- развитие различных форм кооперации (в том числе и международной) в сфере обеспечения информационной безопасности.

1) Приоритет 1. Развитие системы реагирования на происшествия в сфере информационной безопасности предполагает, что быстрое обнаружение атак и своевременный обмен информацией о них во многих случаях могут значительно снизить ущерб. Для обеспечения безопасности Стратегия предполагает реализацию следующих основных мероприятий:

- разработку архитектуры взаимодействия как правительственных, так и неправительственных структур, которая обеспечила бы реагирование на инциденты;
- обеспечение как тактического, так и стратегического анализа атак на информационные ресурсы, а также оценки их уязвимости;
- поощрение распространения частными компаниями имеющейся у них информации об общем состоянии дел в сфере информационной безопасности;
- расширение работы «Информационной сети для предупреждений об угрозах критической инфраструктуре» (CWIN) для поддержки роли Министерства национальной безопасности в разрешении кризисов и некоторых других.

2) Приоритет 2. Реализация программы устранения угроз для информационной безопасности и уязвимостей в информационных системах предполагает, что наличие уязвимостей в различных информационных системах само по себе в определенной мере обуславливает возможность атак на них и, соответственно, является источником опасностей для элементов критически важной инфраструктуры страны. Таким образом, устранение уязвимостей является одним из наиболее важных направлений работы по

обеспечению информационной безопасности. Для обеспечения безопасности Стратегия предполагает реализацию следующих основных мероприятий:

- расширение возможностей проведения расследований компьютерных преступлений для последующего предотвращения возможных атак;
- создание общенационального механизма для оценки уязвимостей с целью обеспечения более полного понимания негативных последствий от реализации угроз и использования уязвимостей;
- повышение безопасности сети Интернет путем совершенствования используемых протоколов и механизмов маршрутизации и некоторых других.

3) Приоритет 3. Развитие ответственного отношения к вопросам информационной безопасности, и подготовка кадров в этой сфере предполагает, что источником многих уязвимостей является недостаточно ответственное отношение некоторых пользователей, системных администраторов и разработчиков информационных систем к вопросам защиты информации, их недостаточная осведомленность и информированность в этой сфере. Для обеспечения безопасности Стратегия предполагает реализацию следующих четырех основных мероприятий:

- продвижение многосторонней общенациональной программы по информированию и развитию ответственного отношения граждан страны к обеспечению безопасности тех информационных систем, к которым они имеют какой-либо доступ;
- поощрение создания программ подготовки специалистов, которые обеспечили бы удовлетворение потребности в персонале;
- повышение эффективности существующих программ подготовки специалистов в сфере информационной безопасности;

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США
(Планирование и управление информационной безопасностью)

- поддержание усилий частных компаний по созданию, распространению и обеспечению всеобщего признания сертификационных программ в сфере информационной безопасности.

4) Приоритет 4. Охрана государственных информационных ресурсов. Для решения задач в этой сфере Стратегия предполагает реализацию следующих основных мероприятий:

- обеспечение непрерывного оценивания угроз для государственных информационных систем и существующих в них (системах) уязвимостей;
- обеспечение безопасности локальных правительственных беспроводных сетей;
- обеспечение безопасности при передаче процессов на аутсорсинг и проведении закупок для правительственных нужд и некоторых других.

5) Приоритет 5. Развитие кооперации между различными ведомствами и компаниями, а также международной кооперации в сфере обеспечения информационной безопасности обусловлено тем, что практически все информационные системы (и в стране, и в мире) являются взаимосвязанными и требуют глобального системного подхода к вопросам защиты информации. Для решения задач в этой сфере Стратегия предполагает реализацию следующих основных мероприятий:

- усиление контрразведывательной деятельности в сферах, имеющих отношение к информационным системам и технологиям;
- поощрение создания национальных и международных сетей наблюдения и предупреждения («watch-and-warning networks»), обеспечивающих выявление и предупреждение атак на информационные ресурсы;
- поощрение присоединения других стран к Конвенции Совета Европы по киберпреступлениям или совершенствования национальных законодательств и некоторых других.

2 Органы планирования и управления информационной безопасностью в США

В соответствии с общей политикой, а также имеющейся базовой инфраструктурой и сложившейся практикой государственного управления в США в течение нескольких лет была организована и постоянно совершенствуется система государственных органов, осуществляющих деятельность в сфере информационной безопасности: были созданы специальные ведомства и расширены задачи и полномочия ранее существовавших. Одним из основных подразделений президентской администрации, специально созданных для решения задач информационной безопасности, является Комитет по национальным системам безопасности (Committee on National Security Systems, CNSS).

Также в системе исполнительной власти были созданы новые отдельные федеральные учреждения, приоритетными задачами которых является решение задач безопасности государства и решение проблем информационной безопасности на федеральном уровне:

1) Министерство национальной безопасности (Department of Homeland Security, DHS), созданное в соответствии с Актом о внутренней безопасности от 25 ноября 2002 г.

2) Управление внутренней безопасности (Office of Homeland Security), созданное Указом Президента США №13228 от 8 октября 2001 г.

3) Совет по внутренней безопасности (Homeland Security Council), также созданный Указом №13228.

Включение функций по обеспечению информационной безопасности в состав функций Министерства национальной безопасности и других аналогичных учреждений объясняется тем, что атаки на информационную инфраструктуру потенциально могут повлечь за собой негативные

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США
(Планирование и управление информационной безопасностью)

последствия для различных жизненно важных отраслей экономики США: финансового сектора, энергетики, транспорта и других.

Кроме того, в рамках отдельных федеральных министерств и ведомств были созданы специальные подразделения, решающие отдельные задачи в рамках общей стратегии обеспечения информационной безопасности США:

1) Группа готовности к чрезвычайным ситуациям в информационных системах – United States Computer Emergency Readiness Team, US-CERT (подразделение, функционирующее в составе DHS);

2) Армейский центр безопасности и поддержки работы глобальных сетей – Army Global Network Operations and Security Center, AGNOSC (подразделение, функционирующее в составе Министерства обороны США);

3) Агентство оборонных информационных систем Министерства обороны США (DISA), под управлением которого находится Объединенный центр обеспечения работы компьютерных сетей – Joint Task Force for Computer Network Operations, JTF-CNO;

4) Центральная служба безопасности (Central Security Service, CSS) Агентства национального безопасности, National Security Agency – NSA.

Таким образом, общая организационная структура государственного управления в сфере информационной безопасности в США является достаточно сложной и состоит из множества относительно самостоятельных и при этом взаимосвязанных элементов, основные из которых представлены на рисунке 1.

Тема 3.4 – Планирование и управление информационной безопасностью на государственном уровне в США
(Планирование и управление информационной безопасностью)

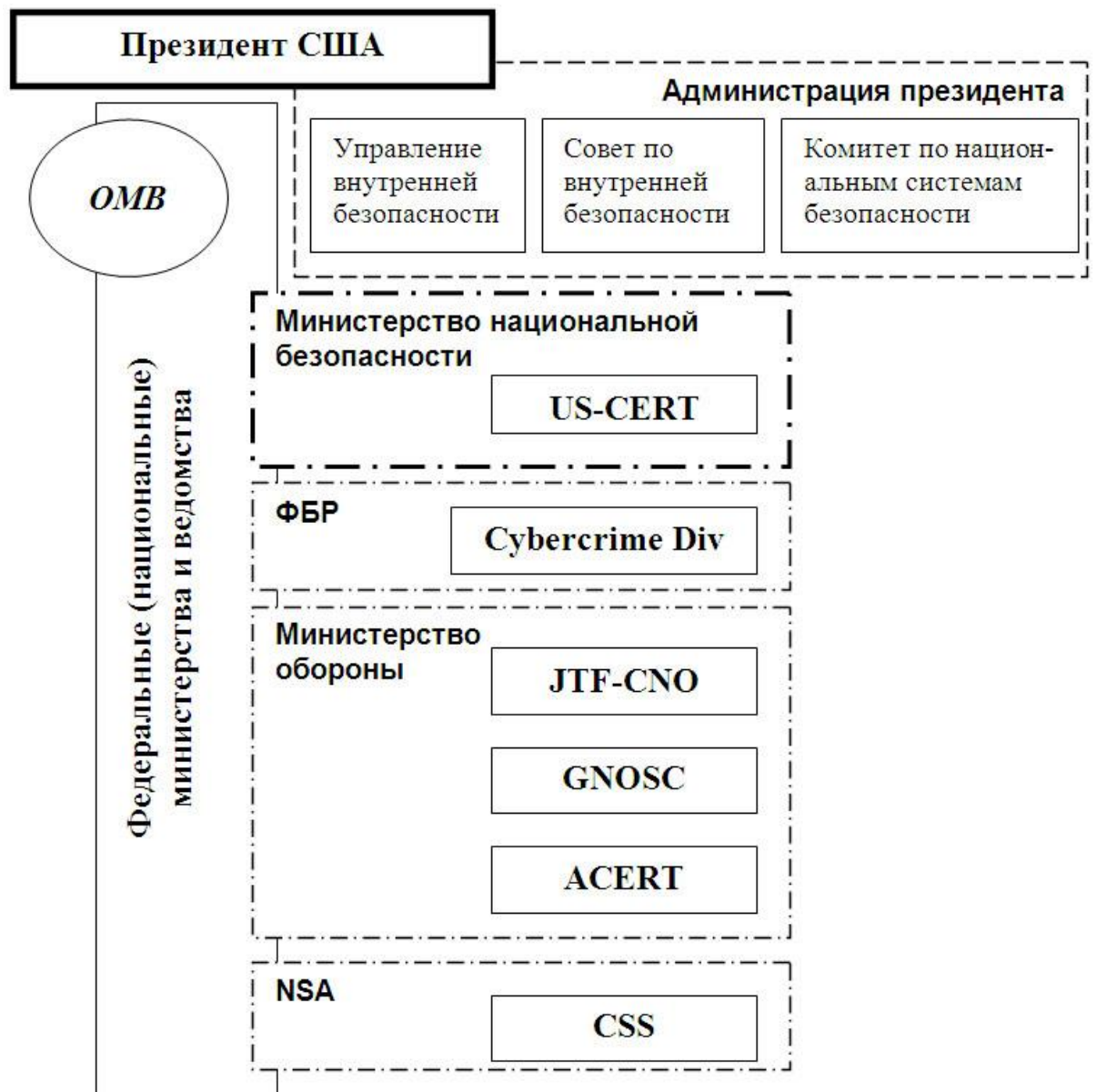


Рисунок 1 – Структура органов управления исполнительной власти УИБ в США

1) Комитет по национальным системам безопасности (Committee on National Security Systems, CNSS) состоит из 21 члена и 11 наблюдателей из числа специалистов различных федеральных ведомств. Работа Комитета ведется в рамках нескольких рабочих групп. Данный комитет формирует централизованную государственную политику в отношении отдельных технологий и методов, важных для защиты информационной инфраструктуры на общенациональном уровне. В частности, работа ведется по таким направлениям, как:

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США

(Планирование и управление информационной безопасностью)

- управление рисками;
- средства идентификации пользователей и устройств;
- устойчивость сетевой инфраструктуры;
- развитие системы подготовки кадров в сфере информационной безопасности;
- обеспечение надежности при расширении совместного доступа к информационным ресурсам.

Основными инструментами достижения целей в данных направлениях являются:

- развитие национальной политики в сфере информационной безопасности, а также разработка стандартов;
- оценка уровня развитости существующих и используемых средств защиты информации;
- выпуск директив, инструкций и технических бюллетеней по определенным проблемам информационной безопасности;
- учреждение новых правительственных структур для решения специализированных задач;
- участие в регулировании экспорта средств защиты информации.

2) Министерство национальной безопасности (Department of Homeland Security, DHS), созданное в ноябре 2002 года в процессе крупнейшей реорганизации государственного аппарата как самостоятельный постоянно действующий орган федеральной власти, наряду с решением различных задач, связанных с безопасностью США (таких как противодействие терроризму и внешним угрозам, а также предотвращение последствий стихийных бедствий), призвано выполнять следующие основные функции в сфере информационной безопасности:

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США

(Планирование и управление информационной безопасностью)

- разработка и совершенствование общенационального плана по обеспечению безопасности ключевых ресурсов и элементов инфраструктуры Соединенных Штатов;
- осуществление управления кризисными ситуациями при атаках на наиболее важные информационные системы;
- предоставление технической поддержки частным компаниям и различным правительственным организациям для устранения последствий сбоев при нарушениях работы критически важных информационных систем;
- координация действий с федеральными структурами в целях своевременного оповещения различных предприятий и организаций о возникающих угрозах и мерах, которые необходимо предпринять;
- выполнение, а также финансирование научно-исследовательских работ, необходимых для решения задач внутренней безопасности.

Функции обеспечения информационной безопасности принадлежат Управлению кибер-безопасности и коммуникаций (Office of Cyber Security and Communications). В составе этого управления функционирует подразделение, непосредственной функцией которого является разрешение проблем, связанных с информационной безопасностью, – National Cyber Security Division, в которое, в свою очередь, включен USCERT.

3) Группа готовности к чрезвычайным ситуациям в информационных системах (United States Computer Emergency Readiness Team, US-CERT) является центральным круглосуточно функционирующим органом, отвечающим за взаимодействие с правительственными структурами (как федеральными, так и местными), а также другими субъектами по вопросам защиты информации. Ее основной обязанностью является сбор и распространение информации с целью реагирования на инциденты, повышения уровня скоординированности действий, снижения уровня уязвимости.

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США
(Планирование и управление информационной безопасностью)

Группа включает в себя пять подразделений.

А) Отдел текущей деятельности (Operations branch). Отвечает за обработку получаемой информации об инцидентах, обеспечивает реагирование на инциденты, распространяет необходимую информацию, а также обеспечивает анализ различных данных с целью повышения качества оценки известных или новых угроз для критически важных элементов национальной инфраструктуры (включая анализ сетевой инфраструктуры, анализ вредоносного ПО и пр.).

Б) Отдел ситуационной информированности (Situational Awareness branch). Отвечает за комплексный анализ сетевой активности (тенденций и характера изменений загрузки магистральных сетей) и информирование федеральных структур с целью повышения уровня их защищенности. Также обеспечивает поддержку в разрешении инцидентов.

В) Следственный отдел (Law Enforcement and Intelligence branch). Обеспечивает взаимодействие с правоохранительными органами при выявлении и расследовании противоправных действий.

Г) Отдел перспективного развития (Future Operation branch). Отвечает за разработку перспективных планов, процедур, регламентов, обеспечивающих работу US-CERT по реагированию на инциденты.

Д) Отдел поддержки (Mission Support branch). Обеспечивает поддержку средств коммуникации, необходимых для работы USCERT, включая поддержку веб-сайта, а также отвечает за административную поддержку, безопасность персонала, снабжение и другие вспомогательные функции.

Помимо обеспечения работы US-CERT, Министерство национальной безопасности также выполняет работу по следующим направлениям:

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США
(Планирование и управление информационной безопасностью)

- проводит периодические (раз в два года) учения Cyber Storm с целью проверки готовности к чрезвычайным ситуациям в сфере информационной безопасности;
- проводит ежегодный информационно-образовательный месячник по кибер-безопасности;
- координирует работу группы из 13 федеральных ведомств (включая разведку, правоохранные структуры и US-CERT) на случай возникновения инцидентов общенационального масштаба;
- поддерживает систему информационного обмена между работниками правоохранительных органов с целью выявления и розыска преступников, совершивших кибер-преступления (Cyber Cop Portal).

4) Агентство оборонных информационных систем (Defense Information Systems Agency, DISA) Министерства обороны США выполняет множество функций, связанных с поддержкой военных информационных систем, и, в частности, функции, связанные с обеспечением их надежности и безопасности.

Директору DISA подчиняется Объединенный центр обеспечения работы компьютерных сетей (Joint Task Force for Computer Network Operations, JTF-CNO¹) Министерства обороны США, который был создан в 1998 году как единый центр координации действий по защите Оборонной информационной инфраструктуры.

Основными задачами JTF-CNO являются:

- обнаружение вторжений в информационные системы подразделений Министерства обороны и других ведомств;
- анализ обнаруженных вторжений в контексте текущей военной обстановки с учетом имеющейся разведывательной информации;
- оценка влияния вторжений на функционирование информационных сетей и военные операции;

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США

(Планирование и управление информационной безопасностью)

- подготовка плана действий по восстановлению работы компьютерных сетей;
- координация необходимых действий с различными подразделениями Министерства обороны и другими ведомствами;
- самостоятельное осуществление конкретных мер по обеспечению безопасности информационных систем.

В состав сил, отвечающих за информационную безопасность армии США, также входят:

- 1) Первое командование информационными операциями американской армии (U.S. Army's 1st Information Operations Command (LAND) (1ST IOC[L])), ранее известное как Подразделение по наземным военным информационным операциям (Land Information Warfare Activity, LIWA).
- 2) Морское командование оборонными операциями в киберпространстве (Navy Cyber Defense Operations Command).
- 3) Армейский центр реагирования на угрозы информационной безопасности (ACERT).

Кроме перечисленных функций органов федеральной власти, государственная политика информационной безопасности также предписывает другим учреждениям оказывать необходимое содействие решению проблем информационной безопасности:

- 1) Национальному научному фонду – оказывать финансовую поддержку научных исследований в сфере информационной безопасности.
- 2) Государственному департаменту – оказывать различным органам необходимое содействие при осуществлении международного сотрудничества в сфере информационной безопасности.
- 3) Центральному разведывательному управлению – противостоять проникновениям в информационные системы из-за рубежа.

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США
(Планирование и управление информационной безопасностью)

4) Национальному институту стандартов (NIST), в лице Управления по компьютерной безопасности, состоящего из четырех групп, – разрабатывать необходимые стандарты в сфере информационной безопасности.

5) Министерству обороны – оказывать техническое содействие при разработке и внедрении систем защиты информации.

6) Министерству юстиции и Федеральному бюро расследований – обеспечивать эффективное расследование и пресечение киберпреступлений, а также осуществлять юридическую поддержку органов федеральной власти при разрешении различных вопросов, связанных с информационной безопасностью.

Также Административно-бюджетное управление (Office of Management and Budget, OMB) уполномочено осуществлять надзор за внедрением мер информационной безопасности (применением политик безопасности, соответствием действующим стандартам, выполнением различных требований и пр.) во всех федеральных органах власти за исключением органов государственной безопасности.

Таким образом, из описания функций различных ведомств, входящих в систему исполнительной власти США, понятно, что часть из них формирует общую политику и координирует действия на уровне министерств, часть – решает вопросы методической и технической поддержки процессов защиты информации, а часть – выполняет повседневную работу, связанную с разрешением отдельных инцидентов и совершенствованием отдельных систем защиты информации.

В составе законодательной ветви власти – Конгресса США – основным структурным подразделением, отвечающим за решение проблем информационной безопасности, является один из 22 постоянных комитетов Палаты представителей – Особый комитет по национальной безопасности

(Select Committee on Homeland Security). Основным профильным подкомитетом является Подкомитет по новым угрозам, кибербезопасности и науке (Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology). В сферу его интересов входят вопросы, связанные с безопасностью компьютерных систем, телекоммуникаций, информационных технологий, систем автоматического управления в промышленности, а также вопросы предотвращения внутренних и внешних атак на правительственные и частные сети, ущерба, нанесенного гражданскому населению вследствие атак на информационные системы.

Некоторые слушания по вопросам информационной безопасности также может проводить Комитет по энергетике и торговле (Committee on Energy and Commerce). В частности, этими проблемами может заниматься Подкомитет по телекоммуникациям и сети Интернет (Subcommittee on Communications, Technologies, and the Internet).

В состав задач Конгресса в сфере управления информационной безопасностью, так же, как и во всех других сферах государственного управления, в соответствии с Конституцией страны входят:

- принятие законодательства;
- принятие бюджета и управление финансами;
- контроль за деятельностью правительственных учреждений;
- выполнение квазисудебных функций;
- формирование структуры исполнительной и судебной власти.

Одной из основных форм работы Конгресса и, в частности, Комитета по национальной безопасности и Комитета по энергетике и торговле, является проведение специальных слушаний и расследований. Слушания проводятся с целью определения направлений совершенствования законодательства, выявления и пресечения недоработок и нарушений в работе органов исполнительной ветви власти и пр. Конгресс может

рассматривать как вопросы, связанные с национальной безопасностью и информационной безопасностью государственных структур, так и проблемы информационной безопасности частного сектора и граждан страны. Для участия в слушаниях по различным вопросам, связанным с информационной безопасностью, в Конгресс, как правило, приглашаются руководители и эксперты, представляющие различные области деятельности:

- представители правительственных учреждений, в чью компетенцию входит обеспечение информационной безопасности (таких как NSA и пр.);
- руководители крупных частных компаний, являющихся лидерами в производстве информационных систем и оказании информационных услуг (таких, как Microsoft, ISS и других);
- представители авторитетных научно-исследовательских учреждений, консалтинговых компаний, профессиональных и отраслевых объединений (таких, как Electronic Industries Alliance).

Деятельность комитетов и подкомитетов Конгресса поддерживается Главным контрольным управлением Конгресса (Government Accountability Office, GAO), в число функциональных подразделений которого входит специальная группа, занимающаяся вопросами информационных технологий и информационной безопасности (Information Technology Team). В список задач этого подразделения включены:

- изучение состояния информационной инфраструктуры и информационной безопасности на разных уровнях и в различных правительственных организациях с целью устранения рисков в их деятельности;
- изучение и продвижение передового опыта («лучших практик») в сфере построения надежных и безопасных информационных систем, а также современных информационных технологий, на основе которых такие системы могут строиться;

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США

(Планирование и управление информационной безопасностью)

- оценка отдельных технологий защиты информации с точки зрения их возможного применения в тех или иных правительственных структурах;
- контроль за обоснованностью бюджетных расходов на обеспечение информационной безопасности;
- изучение возможностей практического развития концепции т.н. «электронного правительства» (e-government).

На основе результатов своей аналитической работы GAO может делать заключения, представлять аналитические материалы заинтересованным конгрессменам, формулировать рекомендации и пр.

3 Федеральные программы и инициативы, поддерживаемые государством

Помимо организации работы отдельных ведомств, одним из важных направлений деятельности государства является поддержка программ совместной деятельности в сфере информационной безопасности всех государственных учреждений, а также частных компаний.

Одной из основных таких инициатив является Межрегиональный Центр обмена и анализа информации (Multi-State Information sharing and analysis center, MS-ISAC), объединяющий структуры, отвечающие за информационную безопасность, в правительствах практически всех штатов. Задачи этого объединения:

- обмен информацией об инцидентах;
- распространение практически опробованных методов и приемов обеспечения безопасности;
- распространение предупреждений о новых угрозах информационной безопасности.

Кроме того, одной из федеральных инициатив является Национальное партнерство по повышению надежности информации – National Information Assurance Partnership, NIAP, созданное для поддержки разработки надежных

Тема 3.4 – Планирование и управление информационной безопасностью на
государственном уровне в США
(Планирование и управление информационной безопасностью)

ИТ-продуктов и проверки информационных систем на соответствие международным стандартам в сфере информационной безопасности. Задачи этой структуры:

- оптимизация расходов правительственных и частных структур на оценку информационных систем;
- поощрение создания частных структур, занимающихся проверкой безопасности информационных продуктов;
- повышение доступности информационных систем, прошедших надлежащую проверку на соответствие современным стандартам.

Также к числу общегосударственных программ относится Информационная сеть для предупреждений об угрозах критической инфраструктуре (Critical infrastructure Warning Information Network, CWIN), основной задачей которой является предоставление возможности обмена предупреждениями и передачи сигналов тревоги между правительственными организациями, а также частными компаниями и некоторыми зарубежными партнерами. По замыслу Министерства национальной безопасности, данная сеть должна обеспечить надежную связь с различными субъектами, чье участие принципиально необходимо для восстановления критически важной инфраструктуры в случае происшествий национального масштаба.