

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

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

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)

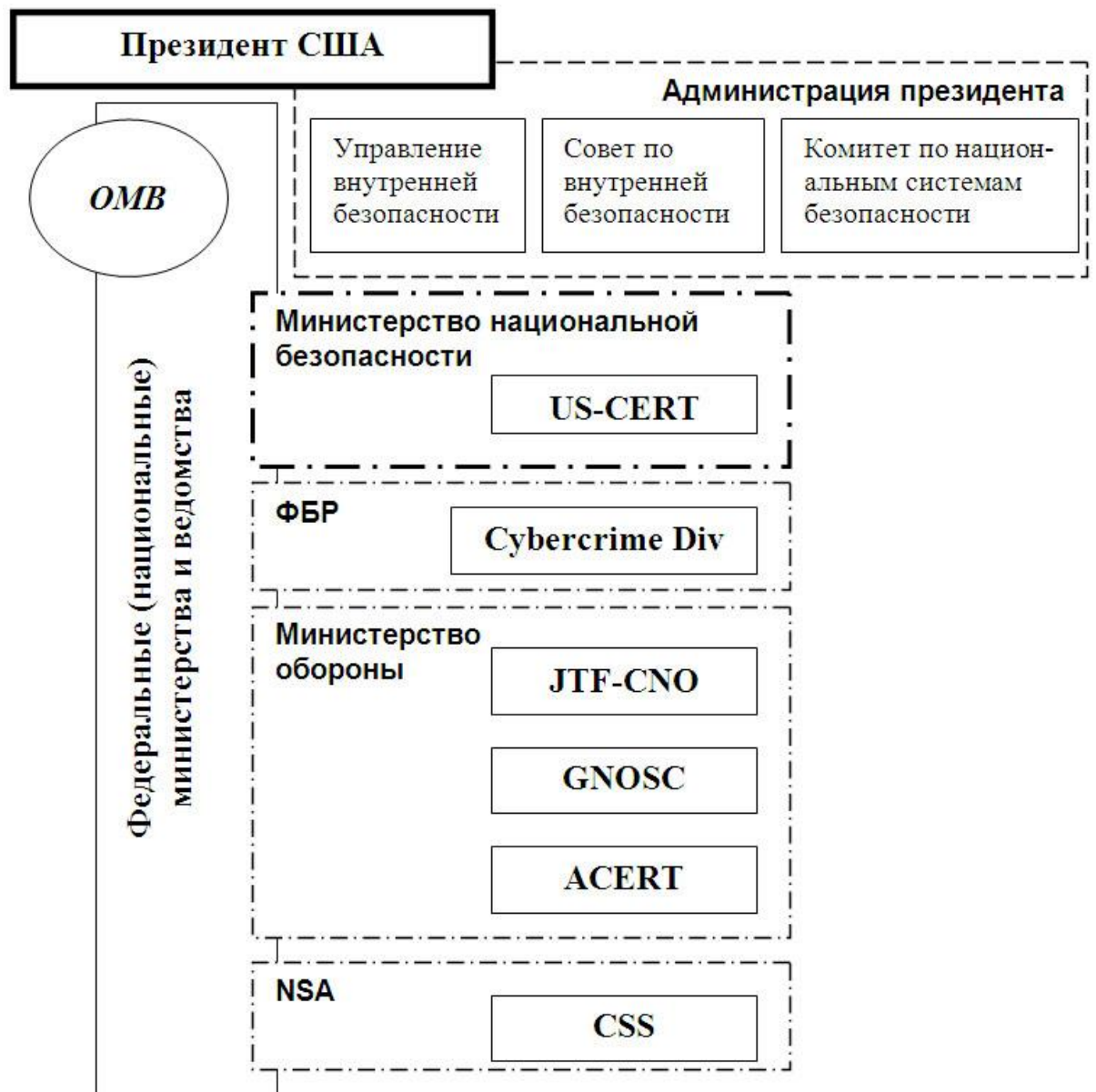


Рисунок 1 – Структура органов управления исполнительной власти УИБ в США

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.

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

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

(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

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

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.