

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 ИТУ-Т 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 ИТУ. Основные рабочие подразделения разделены на три сектора: сектор стандартизации связи, ИТУ-Т; сектор радиосвязи, ИТУ-R; сектор развития электросвязи ИТУ-D.

ИТУ-R и ИТУ-D выполняют отдельные исследовательские, координационные и технические функции (такие как, например, регистрация радиочастот или координация работы космических телекоммуникационных спутников), тогда как Сектор стандартизации связи – ИТУ-Т 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 ИТУ-Т 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).