Оглавление

Предисловие

Познание начинается с удивления.

Аристотель

Быстрое развитие информационных технологий и глобальной сети Интернет привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Корпоративные информационные системы (КИС) становятся сегодня важнейшим средством производства современной компании, они позволяют преобразовать традиционные формы бизнеса в электронный бизнес. Электронный бизнес использует глобальную сеть Интернет и современные информационные технологии для повышения эффективности всех сторон деятельности компаний, включая производство, маркетинг, продажи, платежи, финансовый анализ, поиск сотрудников, поддержку клиентов и партнерских отношений.

Важным условием существования электронного бизнеса является информационная безопасность, под которой понимается защищенность корпоративной информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, способных нанести ущерб владельцам или пользователям информации. Ущерб от нарушения информационной безопасности может привести к крупным финансовым потерям и даже к полному закрытию компании. Поэтому проблемы обеспечения информационной безопасности привлекают внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей, включая компании, работающие в сфере электронного бизнеса. Задача обеспечения безопасности корпоративных информационных систем решается путем построения комплексной системы информационной безопасности.

Без знания и квалифицированного применения современных информационных технологий, стандартов, протоколов и средств защиты информации невозможно достигнуть требуемого уровня информационной безопасности компьютерных систем и сетей.

Предлагаемая вниманию читателя книга посвящена систематическому изложению и анализу современных методов, средств и технологий комплексной защиты информации в корпоративных системах.

Содержимое книги разбито на четыре логически связанных части:

- часть I «Проблемы информационной безопасности»;
- часть II «Технологии защиты данных»;
- часть III «Многоуровневая защита корпоративных информационных систем»;
- часть IV «Управление информационной безопасностью».

Каждая из этих частей объединяет несколько глав, связанных общей темой. Каждая глава завершается набором вопросов для самоконтроля. Книга содержит также список сокращений и список литературы.

Часть I «Проблемы информационной безопасности» включает следующие главы:

- глава 1 «Основные понятия и анализ угроз информационной безопасности»;
- глава 2 «Политика информационной безопасности»;
- глава 3 «Стандарты информационной безопасности».

В главе 1 формулируются основные понятия и определения информационной безопасности и анализируются угрозы информационной безопасности в корпоративных системах и сетях, рассматриваются тенденции развития ИТ-угроз и криминализация атак, формулируются способы обеспечения информационной безопасности и возможные пути решения проблем защиты информации в сетях.

В главе 2 определяются базовые понятия политики безопасности и описываются основные виды политик и процедур безопасности в корпоративных информационных системах.

Глава 3 посвящена описанию стандартов информационной безопасности. Рассматриваются основные международные стандарты информационной безопасности. Даны краткие описания популярных стандартов информационной безопасности для Интернета. Описываются отечественные стандарты безопасности информационных технологий.

Часть II «Технологии защиты данных» включает следующие главы:

- глава 4 «Криптографическая защита информации»;
- глава 5 «Идентификация, аутентификация и управление доступом».

В главе 4 описываются такие криптографические методы защиты корпоративной информации, как симметричные и асимметричные криптосистемы шифрования, комбинированные криптосистемы, электронная цифровая подпись, функции хэширования и управление криптоключами. Подробно рассматривается инфраструктура управления открытыми ключами PKI (Public Key Infrastructure).

Глава 5 посвящена рассмотрению идентификации, аутентификации и авторизации пользователя. Описываются методы аутентификации, использующие многоразовые и одноразовые пароли, протоколы строгой аутентификации, смарт-карты и USB-токены, биометрическую аутентификацию пользователей, управление доступом по схеме однократного входа Single Sign-On.

Часть III «Многоуровневая защита корпоративных информационных систем» объединяет следующие главы:

- глава 6 «Принципы многоуровневой защиты корпоративной информации»;
- глава 7 «Обеспечение безопасности операционных систем»;
- глава 8 «Протоколы защищенных каналов»;
- глава 9 «Технологии межсетевого экранирования»;
- глава 10 «Технологии виртуальных защищенных сетей VPN»;
- глава 11 «Защита удаленного доступа»;
- глава 12 «Технологии обнаружения и предотвращения вторжений»;
- глава 13 «Технологии защиты от вредоносных программ и спама».

Глава 6 посвящена рассмотрению принципов комплексной многоуровневой защиты информации в корпоративных информационных системах. Анализируются традиционные структуры корпоративных информационных систем и инфраструктура «облачных» вычислений. Описывается стратегия многоуровневой защиты КИС. Рассматривается безопасность «облачных» вычислений.

В главе 7 анализируются угрозы безопасности в операционных системах (ОС), вводится понятие защищенной ОС, описываются архитектура и основные функции подсистемы защиты ОС. Рассматриваются средства обеспечения безопасности операционных систем UNIX и Windows 7.

В главе 8 обсуждаются проблемы построения защищенных виртуальных каналов на канальном, сетевом и сеансовом уровнях эталонной модели взаимодействия открытых систем OSI. Рассматриваются особенности применения протоколов на канальном уровне PPTP, L2F и L2TP. Описываются архитектура стека протоколов IPSec, протокол аутентификации AH, протокол формирования защищенного пакета ESP, протокол управления криптоключами IKE. Приводятся сведения об алгоритмах аутентификации и шифрования, применяемых в стеке протоколов IPSec. Описывается применение протоколов SSL и SOCKS для построения защищенных каналов на сеансовом уровне. Рассматривается защита беспроводных сетей.

В главе 9 рассматриваются функции межсетевых экранов. Описываются схемы сетевой защиты на базе межсетевых экранов. Рассматривается применение персональных и распределенных сетевых экранов.

Глава 10 посвящена рассмотрению защищенных виртуальных сетей VPN (Virtual Private Network). Поясняется главное свойство сети VPN – туннелирование. Анализируются варианты построения виртуальных защищенных каналов. Рассматриваются варианты архитектуры сетей VPN и приводятся основные виды технической реализации VPN.

В главе 11 рассматривается организация защищенного удаленного доступа, анализируются протоколы аутентификации и системы централизованного контроля удаленного доступа. Особое внимание уделяется протоколу аутентификации Kerberos.

Глава 12 посвящена проблемам обнаружения и предотвращения вторжений. Рассматриваются методы обнаружения и предотвращения вторжений в корпоративные информационные системы, а также защита от распределенных атак.

В главе 13 описываются технологии защиты от вредоносных программ и спама. Приводится классификация вредоносных программ. Рассматриваются сигнатурный анализ и проактивные методы обнаружения вирусов и других вредоносных программ. Описывается защита корпоративной информационной системы от вредоносных программ.

Часть IV «Управление информационной безопасностью» объединяет следующие главы:

- глава 14 «Управление средствами обеспечения информационной безопасности»;
- глава 15 «Обзор современных систем управления безопасностью».

В главе 14 рассматриваются методы управления средствами защиты корпоративной информации. Сформулированы задачи управления системой информационной безопасности масштаба предприятия. Анализируются варианты архитектуры управления средствами безопасности. Особое внимание уделяется перспективной архитектуре централизованного управления безопасностью на базе глобальной и локальной политик безопасности.

В главе 15 приводится обзор современных систем управления информационной безопасностью. Рассматриваются продукты компаний ЭЛВИС+, Cisco Systems, IBM и Check Point для управления средствами безопасности.

Материал книги базируется только на открытых публикациях в Интернете, отечественной и зарубежной печати. В основу книги положены материалы лекций, читаемых автором в Московском государственном институте электронной техники.

Автор заранее благодарен читателям, которые пришлют ему свои замечания и пожелания по адресу shanico@mail.ru.

Введение

Кто владеет информацией,
тот владеет миром.

Уинстон Черчилль

Деятельность современной компании невозможна без использования информационных технологий. Эффективное применение информационных технологий является общепризнанным фактором конкурентоспособности компании. Многие предприятия в мире переходят к использованию широких возможностей Интернета и электронного бизнеса. Корпоративные информационные системы (КИС) становятся сегодня одним из главных инструментов управления бизнесом и фактически важнейшим средством производства современной компании. В таких условиях одним из наиболее ценных ресурсов организации является корпоративная информация.

Все больше корпоративных систем, приложений и данных становятся доступными из Глобальной сети, вследствие чего компании сталкиваются с возрастающим числом различных угроз для своей информационной инфраструктуры – несанкционированный доступ, вирусная опасность, атаки типа «отказ в обслуживании» и другие виды вторжений, мишенью для которых становятся приложения, компьютерные сети и инфраструктура КИС.

Поэтому применение информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности. Одной из самых актуальных задач, которая стоит сегодня перед разработчиками и поставщиками информационных технологий, является решение проблем информационной безопасности, связанных с широким распространением Интернета, интранета и экстранета.

Реализация решений для электронного бизнеса должна обеспечивать хорошую защиту, конфиденциальность транзакций, предоставлять защиту целостности выполнения деловых операций и данных заказчиков, а также гарантировать постоянный доступ к данным. Информация должна быть доступна только тем, кому она предназначена, и скрыта от сторонних наблюдателей. Несанкционированное использование информационного ресурса, его временная недоступность или раз-

рушение могут нанести компании значительный материальный ущерб. Надежная защита информационных ресурсов повышает эффективность всего процесса информатизации, обеспечивая безопасность дорогостоящей деловой информации, циркулирующей в локальных и глобальной информационных средах.

Использование Интернета в качестве глобальной публичной сети означает для средств безопасности предприятия не только резкое увеличение количества внешних пользователей и разнообразие типов коммуникационных связей, но и сосуществование с новыми сетевыми и информационными технологиями. Поэтому информационные ресурсы и средства осуществления электронных сетевых транзакций (серверы, маршрутизаторы, серверы удаленного доступа, каналы связи, операционные системы, базы данных и приложения) нужно защищать особенно надежно и качественно.

Следует заметить, что средства взлома компьютерных сетей и хищения информации развиваются так же быстро, как и все высокотехнологичные компьютерные отрасли. В этих условиях обеспечение информационной безопасности КИС является приоритетной задачей, поскольку от сохранения конфиденциальности, целостности и доступности корпоративных информационных ресурсов во многом зависит эффективность работы КИС.

Задача обеспечения информационной безопасности КИС традиционно решается построением *системы информационной безопасности* (СИБ), определяющим требованием к которой является сохранение вложенных в построение КИС инвестиций. Иначе говоря, СИБ должна функционировать абсолютно прозрачно для уже существующих в КИС приложений и быть полностью совместимой с используемыми в КИС сетевыми технологиями.

Создаваемая система информационной безопасности предприятия должна учитывать появление новых технологий и сервисов, а также удовлетворять общим требованиям, предъявляемым сегодня к корпоративной информационной системе:

- применение открытых стандартов;
- использование интегрированных решений;
- обеспечение масштабирования в широких пределах.

Переход на открытые стандарты составляет одну из главных тенденций развития современных средств информационной безопасности. Такие стандарты, как IPSec и PKI, обеспечивают защищенность внешних коммуникаций предприятий и совместимость с соответствующими продуктами предприятий-партнеров или удаленных клиентов. Цифровые сертификаты X.509 также являются на сегодня стандартной основой для аутентификации пользователей и устройств. Современные и перспективные средства защиты, безусловно, должны поддерживать эти стандарты.

Под *интегрированными решениями* понимаются как интеграция средств защиты с остальными элементами сети (операционными системами, маршрутизаторами, службами каталогов, серверами QoS-политики и т. п.), так и интеграция различных технологий безопасности между собой для обеспечения *комплексной защиты*

информационных ресурсов предприятия, например интеграция межсетевого экрана с VPN-шлюзом и транслятором IP-адресов.

По мере роста и развития КИС система информационной безопасности должна иметь возможность легко масштабироваться без потери целостности и управляемости. *Масштабируемость средств защиты* позволяет подбирать оптимальное по стоимости и надежности решение с возможностью постепенного наращивания системы защиты. Масштабирование обеспечивает эффективную работу предприятия при наличии у него многочисленных филиалов, десятков предприятий-партнеров, сотен удаленных сотрудников и миллионов потенциальных клиентов.

Для того чтобы обеспечить надежную защиту ресурсов корпоративной информационной системы, в системе информационной безопасности должны быть реализованы самые прогрессивные и перспективные технологии информационной защиты. К ним относятся:

- *криптографическая защита данных* для обеспечения конфиденциальности, целостности и подлинности информации;
- *поддержка инфраструктуры управления открытыми ключами PKI*;
- *технологии аутентификации* для проверки подлинности пользователей и объектов сети путем применения одноразовых паролей, токенов (смарт-карт, USB-токенов) и других средств аутентификации;
- *управление доступом на уровне пользователей* и защита от несанкционированного доступа к информации;
- *комплексный многоуровневый подход к построению системы информационной безопасности*, обеспечивающий рациональное сочетание технологий и средств информационной защиты;
- *технологии межсетевых экранов* для защиты корпоративной сети от внешних угроз при подключении к общедоступным сетям связи;
- *технологии виртуальных защищенных каналов и сетей VPN* для защиты информации, передаваемой по открытым каналам связи;
- *технологии обнаружения и предотвращения вторжений в КИС*;
- *технологии защиты от вредоносных программ и спама* с использованием комплексов антивирусной защиты;
- *обеспечение безопасности «облачных» вычислений*;
- *централизованное управление средствами информационной безопасности* на базе единой политики безопасности предприятия.

Предлагаемая книга дает читателю достаточно полное представление о современных и перспективных методах, средствах и технологиях защиты информации в корпоративных системах и сетях. Книга представляет интерес для пользователей и администраторов компьютерных сетей и систем, менеджеров, руководителей предприятий, заинтересованных в безопасности своих корпоративных информационных систем и сетей.

Данная книга может быть полезна в качестве учебного пособия для студентов вузов, обучающихся по направлению «Информатика и вычислительная техника», а также для аспирантов и преподавателей соответствующих специальностей.

Список сокращений

3-DES (Triple Data Encryption Standard) – алгоритм тройного шифрования, разновидность алгоритма DES.
ACK (Acknowledgement) – подтверждение.
AES (Advanced Encryption Standard) – американский стандарт шифрования данных.
AH (Authentication Header) – аутентифицирующий заголовок в IPSec.
AP (Access Point) – точка доступа – коммуникационный узел для пользователей или беспроводное устройство.
AS (Authentication Server) – сервер аутентификации.
ASA (Adaptive Security Algorithm) – алгоритм адаптивной безопасности.
B2B (Business-to- Business) – схема бизнес–бизнес: модель ведения бизнеса в Интернете на уровне компаний.
B2C (Business-to-Consumer) – схема бизнес–потребитель: розничная продажа товаров и услуг частным лицам через Интернет.
CA (Certification Authority) – центр сертификации.
CEK (Content Encryption Key) – ключ шифрования данных.
CHAP (Challenge-Handshake Authentication Protocol) – протокол аутентификации на основе процедуры запрос–отклик.
CRL (Certificate Revocation List) – список аннулированных сертификатов.
CSA (Cloud Security Alliance) – альянс в сфере облачной безопасности.
DDoS (Distributed Denial of Service) – распределенная атака отказа в обслуживании.
DES (Data Encryption Standard) – бывший стандарт шифрования данных США.
DH (Diffie–Hellman) – Диффи–Хеллман.
DHCP (Dynamic Host Configuration Protocol) – протокол динамической конфигурации хостов.
DMZ (Demilitarized Zone) – демилитаризованная зона, безопасная зона сети.
DNS (Domain Name Server) – служба имен доменов.
DOI (Domain of Interpretation) – область интерпретации.

DoS (Denial of Service) – атака отказа в обслуживании.
DSSS (Direct Sequence Spread Spectrum) – распределенный спектр с прямой последовательностью.
EAP (Extensible Authentification Protocol) – расширяемый протокол аутентификации.
ECC (Elliptic Curve Cryptography) – криптография эллиптических кривых.
EE (End Entity) – конечный пользователь.
EEPROM (Electrically Erasable Programmable Read-only Memory) – электрически программируемая память только для чтения данных.
ESP (Encapsulated Security Payload) – встроенная полезная нагрузка безопасности для IPSec.
FHSS (Frequency Hopping Spread Spectrum) – распределенный спектр со скачками по частотам.
FTP (File Transfer Protocol) – протокол передачи файлов.
GPS (Global Positioning System) – система глобального позиционирования.
GSP (Global Security Policy) – глобальная политика безопасности для всей VPN.
HMAC (Hashing for Message Authentication) – аутентификация сообщений с хэшированием по ключам.
HTTP (HyperText Transfer Protocol) – протокол передачи гипертекстовых файлов.
ICMP (Internet Control Message Protocol) – протокол управляющих сообщений в сети Интернет.
ICV (Integrity Check Value) – значение проверки целостности.
IDS (Intrusion Detection System) – система определения вторжений.
IEEE (Institute of Electrical and Electronics Engineers) – Институт инженеров по электротехнике и радиоэлектронике.
IEEE 802.11 – группа разработки стандартов в IEEE, цель которой – выпуск стандартов беспроводных локальных сетей LAN.
IKE (Internet Key Exchange) – протокол обмена ключами в Интернете.
IP (Internet Protocol) – интернет-протокол межсетевого обмена данными.
IPS (Intrusion Prevention System) – система предотвращения вторжений.
IPSec (Internet Security Protocol) – интернет-протокол безопасного межсетевого обмена.
IPv4 (Internet Protocol, version 4) – интернет-протокол межсетевого обмена, версия 4.
IPv6 (Internet Protocol, version 6) – интернет-протокол межсетевого обмена, версия 6.
ISAKMP (Internet Security Association and Key Management Protocol) – протокол безопасных ассоциаций и управления ключами Интернета.
ISDN (Integrated Services Digital Network) – цифровые сети с интегральными услугами.
ISO (International Standards Organization) – Международная организация по стандартизации.

ISP (Internet Service Provider) – поставщик услуг Интернета.
IT (Information Technology) – информационная технология.
KEK (Key-Encryption Key) – ключ для шифрования ключей.
KS (Kerberos Server) – сервер системы Kerberos.
L2F (Layer-2 Forwarding) – протокол передачи данных второго (канального) уровня.
L2TP (Layer-2 Tunneling Protocol) – протокол туннелирования данных второго (канального) уровня.
LAC (L2TP Access Concentrator) – концентратор доступа L2TP.
LAN (Local Access Network) – локальная сеть.
LCP (Link Control Protocol) – протокол управления соединением.
LDAP (Lightweight Directory Access Protocol) – облегченный протокол доступа к каталогам.
LNS (L2TP Network Server) – сетевой сервер L2TP.
LSP (Local Security Policy) – локальная политика безопасности (для клиента).
MAC (Media Access Control) – управление доступом к среде.
MAC (Message Authentication Code) – код аутентификации сообщения.
MAN (Metropolitan Area Network) – городская сеть.
MD (Message Digest) – дайджест сообщения.
MIB (Management Information Base) – стандарт базы данных для управления сетью.
MIF (Management Information File/ Format) – формат для файлов управляющей информации.
MITM (Man In The Middle) – сетевая атака «человек-в-середине».
MTU (Maximum Transmission Unit) – максимальный размер передаваемого блока.
NAK (Negative Acknowledgement) – подтверждение отказа.
NAS (Network Access Server) – сервер доступа к сети.
NAT (Network Address Translation) – трансляция сетевых адресов.
NCP (Network Control Protocol) – протокол управления сетью.
NIDS (Network-based Intrusion Detection System) – система обнаружения вторжений в сеть.
NNM (Network Node Manager) – система сетевого управления.
OCSP (Online Certificate Status Protocol) – протокол статуса текущего сертификата.
OSI (Open Systems Interconnection) – взаимодействие открытых систем.
OTK (One-Time Key) – одноразовый ключ.
OTP (One-Time Password) – одноразовый пароль.
PAP (Password Authentication Protocol) – протокол аутентификации по паролю.
PDA (Personal Digital Assistant) – карманный персональный компьютер, КПК.
PGP (Pretty Good Privacy) – достаточно хорошая секретность.

PKD (Public Key Directory) – каталог открытых ключей.
PKI (Public Key Infrastructure) – инфраструктура управления открытыми ключами.
PPP (Point-to-Point Protocol) – протокол двухточечного соединения.
PPTP (Point-to-Point Tunneling Protocol) – протокол туннелирования для двухточечного соединения.
QOS (Quality of Service) – качество предоставляемых услуг.
RADIUS (Remote Authentication Dial-In User Service) – система удаленной аутентификации пользователей по коммутируемым линиям.
RAS (Remote Access Service) – служба удаленного доступа.
RC4 (Rivest Cipher 4) – потоковый шифр, разработанный Роном Райвестом и используемый в базовом стандарте IEEE 802.11.
RFC (Request For Comments) – запрос комментариев.
RFID (Radio Frequency Identifier) – радиочастотный идентификатор.
RPC (Remote Procedure Call) – удаленный вызов процедуры.
RSA (Rivest–Shamir–Adleman) – Райвест–Шамир–Эйдельман.
SA (Security Associations) – безопасные ассоциации.
SAD (Security Associations Database) – база данных безопасных ассоциаций.
SET (Secure Electronic Transaction) – стандарт защищенных электронных транзакций.
SHA-1 (Secure Hash Algorithm) – алгоритм защищенного хэширования версии 1, широко используемый в США.
SHA-2 (Secure Hash Algorithm Version 2) – алгоритм защищенного хэширования версии 2, обозначающий семейство более стойких хэш-функций SHA-224, SHA-256, SHA-384 и SHA-512 с длинами хэша соответственно 224, 256, 384 и 512 бит.
SKIP (Simple Key management for Internet Protocols) – простое управление ключами для интернет-протоколов.
SMTP (Simple Mail Transfer Protocol) – простой протокол электронной почты.
SNMP (Simple Network Management Protocol) – простой протокол сетевого управления.
SOHO (Small Office / Home Office) – решения для малых и домашних офисов.
SPD (Security Policy Database) – база данных правил безопасности.
SPI (Security Parameter Index) – индекс параметров защиты.
SQL (Structured Query Language) – структурированный язык запросов.
SSH (Secure Shell) – безопасный уровень. Протокол и программа SSH обеспечивают надежные шифрование и аутентификацию.
SSL (Secure Sockets Layer) – уровень безопасных соединений. Протокол для установки шифрованных соединений между интернет-сервером и интернет-браузером.
TACACS (Terminal Access Controller Access Control System) – протокол централизованного контроля удаленного доступа.