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.

TCP (Transport Control Protocol) – протокол управления передачей.
TGS (Ticket Granting Server) – сервер выдачи разрешений.
TLS (Transport Layer Security) – защита транспортного уровня.
UDP (User Data Protocol) – протокол передачи данных пользователя.
URL (Uniform Resource Locator) – унифицированный указатель ресурса.
VPN (Virtual Private Network) – защищенная виртуальная сеть.
WAN (Wide Area Network) – сеть, развернутая на большой территории.
WWW (World Wide Web) – служба гипертекстовой информации Интернета.

ЧАСТЬ I

Проблемы информационной безопасности

Корпоративные информационные системы (КИС) становятся сегодня одним из главных инструментов управления бизнесом и фактически важнейшим средством производства современной компании. Однако применение информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности. Разрушение информационного ресурса, его временная недоступность или несанкционированное использование могут нанести компании значительный материальный ущерб. Без должной степени защиты информации внедрение информационных технологий может оказаться экономически невыгодным в результате значительного ущерба из-за потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях.

Корпоративная информационная система представляет собой сложный комплекс разнородного аппаратного и программного обеспечения: компьютеров, операционных систем, сетевых средств, СУБД, разнообразных приложений. Все эти компоненты обычно обладают собственными средствами защиты, которые нужно согласовать между собой. Поэтому очень важна эффективная политика безопасности в качестве согласованной платформы по обеспечению безопасности корпоративной системы.

В последние годы в связи с развитием компьютерных сетей и ростом спроса на электронные услуги ситуация в сфере информационной безопасности серьезно обострилась, а вопрос стандартизации подходов к решению проблемы информационной безопасности стал особенно актуальным.

Реализация решений, обеспечивающих безопасность информационных ресурсов, существенно повышает эффективность всего процесса информатизации в организации, обеспечивая целостность, подлинность и конфиденциальность важной деловой информации, циркулирующей в локальных и глобальной информационных средах.

ГЛАВА 1 Основные понятия и анализ угроз информационной безопасности

Непостижимо все, что в мире есть.
К тому ж изъянов в том, что есть, не счесть.

Омар Хайям «Рубаи»

Новые информационные технологии активно внедряются во все сферы человеческой деятельности. Появление локальных и глобальных сетей передачи данных предоставило пользователям компьютеров новые возможности для оперативного обмена информацией. Развитие Интернета привело к использованию глобальных сетей передачи данных в повседневной жизни практически каждого человека. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий.

1.1. Основные понятия информационной безопасности и защиты информации

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Рассмотрим основные понятия информационной безопасности и защиты информации компьютерных систем и сетей с учетом определений стандарта ГОСТ Р 50922-96 [10, 45].

Под *информационной безопасностью* понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищен-

ность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной. Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, и стихийные бедствия (землетрясение, ураган, пожар и т. п.).

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты – информация, или носитель информации, или информационный процесс, в отношении которого необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации – это желаемый результат защиты информации. Целью защиты информации может быть предотвращение нанесения ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на нее.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки – деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к ней и от получения защищаемой информации злоумышленниками.

Защита информации от несанкционированного воздействия – деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия – деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информации, сбоя технических и программных средств информационных систем, а также природных явлений или иных не направленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, которые приводят к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения – деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от несанкционированного доступа (*НСД*) – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим несанкционированный

доступ к защищаемой информации, может выступать государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Система защиты информации – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, которые установлены соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Современная *автоматизированная информационная система* (*ИС*) представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. *Компоненты ИС* можно разбить на следующие группы:

- *аппаратные средства* – компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – дисководы, принтеры, контроллеры, кабели, линии связи и т. д.);
- *программное обеспечение* – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;
- *данные* – информация, хранимая временно и постоянно на магнитных носителях, печатная, архивы, системные журналы и т. д.;
- *персонал* – обслуживающий персонал и пользователи.

Одной из особенностей обеспечения информационной безопасности в ИС является то, что таким абстрактным понятиям, как информация, объекты и субъекты системы, ставятся в соответствие физические представления в компьютерной среде:

- *для представления информации – машинные носители информации* в виде внешних устройств компьютерных систем (терминалов, печатающих устройств, различных накопителей, линий и каналов связи), оперативной памяти, файлов, записей и т. д.;
- под *объектами системы* понимают пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем информации;
- под *субъектами системы* понимают активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы.

Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

Перечисленные выше *базовые свойства информации* нуждаются в более полном толковании.

Конфиденциальность данных – это статус, предоставленный данным и определяющий требуемую степень их защиты. К конфиденциальным данным можно отнести, например, следующие: личную информацию пользователей; учетные записи (имена и пароли); данные о кредитных картах; данные о разработках и различные внутренние документы; бухгалтерские сведения. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Установление градаций важности защиты защищаемой информации (объекта защиты) называют *категорированием защищаемой информации*.

Под *целостностью информации* понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, то есть если не произошло их случайного или преднамеренного искажения или разрушения. Обеспечение целостности данных является одной из сложных задач защиты информации.

Достоверность информации – свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Юридическая значимость информации означает, что документ, являющийся носителем информации, обладает юридической силой.

Доступность данных – работа пользователя с данными возможна только в том случае, если он имеет к ним доступ.

Доступ к информации – получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Субъект доступа к информации – участник правоотношений в информационных процессах.

Оперативность доступа к информации – это способность информации или некоторого информационного ресурса быть доступными для конечного пользователя в соответствии с его оперативными потребностями.

Собственник информации – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Владелец информации – субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Пользователь (*потребитель*) *информации* – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Право доступа к информации – совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации.

Правило доступа к информации – совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации – это доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ (*НСД*) к информации характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений.

Ответственным за защиту компьютерной системы от несанкционированного доступа к информации является *администратор защиты.*

Доступность информации подразумевает также *доступность компонента или ресурса* компьютерной системы, то есть свойство компонента или ресурса быть доступным для законных субъектов системы. Вот примерный перечень ресурсов, которые должны быть доступны: принтеры; серверы; рабочие станции; данные пользователей; любые критические данные, необходимые для работы.

Целостность ресурса или компонента системы – это свойство ресурса или компонента быть неизменными в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений либо разрушающих воздействий.

С допуском к информации и ресурсам системы связана группа таких важных понятий, как идентификация, аутентификация, авторизация.

С каждым субъектом системы (сети) связывают некоторую информацию (число, строку символов), идентифицирующую субъект, Эта информация является *идентификатором* субъекта системы (сети). Субъект, имеющий зарегистрированный идентификатор, является *законным* (*легальным*) *субъектом.*

Идентификация субъекта – это процедура распознавания субъекта по его идентификатору. Идентификация выполняется при попытке субъекта войти в систему (сеть).

Следующим шагом взаимодействия системы с субъектом является аутентификация субъекта.

Аутентификация субъекта – это проверка подлинности субъекта с данным идентификатором. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил.

После идентификации и аутентификации субъекта выполняют процедуру авторизации.

Авторизация субъекта – это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Под *угрозой безопасности* ИС понимаются возможные действия, способные прямо или косвенно нанести ущерб ее безопасности. *Ущерб безопасности* под-

разумевает нарушение состояния защищенности информации, содержащейся и обрабатываемой в системе (сети).

С понятием угрозы безопасности тесно связано понятие уязвимости компьютерной системы (сети). *Уязвимость компьютерной системы* – это присущее системе неудачное свойство, которое может привести к реализации угрозы.

Атака на компьютерную систему – это поиск и/или использование злоумышленником той или иной уязвимости системы. Иными словами, атака – это реализация угрозы безопасности.

Противодействие угрозам безопасности является целью средств защиты компьютерных систем и сетей.

Защищенная система – это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные либо используемые для защиты информации.

Комплекс средств защиты (*КСЗ*) представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы (сети). КСЗ создается и поддерживается в соответствии с принятой в данной организации политикой безопасности.

Техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Корпоративные сети относятся к распределенным информационным системам (ИС), осуществляющим обработку информации. Обеспечение безопасности ИС предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования ИС, а также попыткам модификации, хищения, выведения из строя или разрушения ее компонентов, то есть защиту всех компонентов ИС – аппаратных средств, программного обеспечения, данных и персонала. Конкретный подход к проблеме обеспечения безопасности основан на политике безопасности, разработанной для ИС.

Политика безопасности – это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы от заданного множества угроз. Более подробные сведения о видах политики безопасности и процессе ее разработки приводятся в главе 2.

1.2. Анализ угроз информационной безопасности

Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе защиты. Обычно под *угрозой* (в общем смысле) понимают потенциально возможное со-

бытие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам. Далее под *угрозой безопасности* информационной системы будем понимать возможность воздействия на ИС, которое прямо или косвенно может нанести ущерб ее безопасности.

В настоящее время известен достаточно обширный перечень угроз безопасности ИС, содержащий сотни позиций. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты ИС. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Необходимость классификации угроз безопасности ИС обусловлена тем, что хранимая и обрабатываемая информация в современных ИС подвержена воздействию чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Поэтому для защищаемой системы обычно определяют не полный перечень угроз, а перечень классов угроз.

Принято считать, что, вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации, ИС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие важные свойства информации и систем ее обработки: *доступность, целостность и конфиденциальность информации*. Иными словами, информационная безопасность ИС обеспечена в случае, если для информационных ресурсов в системе поддерживаются определенные уровни:

- доступности (возможности за разумное время получить требуемую информацию);
- целостности (невозможности несанкционированной или случайной модификации информации);
- конфиденциальности (невозможности несанкционированного получения информации).

Соответственно, для автоматизированных информационных систем угрозы следует классифицировать прежде всего по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого они направлены в первую очередь:

- *угрозы нарушения доступности (отказ в обслуживании)*, направленные на создание таких ситуаций, когда определенные действия либо блокируют доступ к некоторым ресурсам ИС, либо снижают ее работоспособность. Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным;