Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
Московский государственный институт электронной техники
(технический университет)

В.Ф. Шаньгин

Комплексная защита корпоративной информации

Учебное пособие

Допущено Учебно-методическим объединением вузов
по университетскому политехническому образованию
в качестве учебного пособия для студентов высших
учебных заведений, обучающихся по направлению
230100 «Информатика и вычислительная техника»

Москва 2009

УДК 004.056
Ш20

Рецензенты: канд. техн. наук, доц. *А.А. Петров*,
докт. техн. наук, проф. *Б.Г. Трусов*

Шаньгин В.Ф.

Ш20 Комплексная защита корпоративной информации: Уч. пособие. - М.: МИЭТ, 2009. - 404 с.: ил.
ISBN 978-5-7256-0537-2

Рассматриваются методы и средства комплексной защиты информации в корпоративных системах. Формулируются основные понятия защиты информации, анализируются угрозы информационной безопасности в корпоративных системах. Обсуждаются базовые понятия и принципы политики безопасности. Обосновывается комплексный подход к обеспечению информационной безопасности корпоративных систем. Описываются криптографические методы и алгоритмы защиты корпоративной информации. Обсуждаются методы и средства идентификации, аутентификации и управления доступом в корпоративных системах. Рассматривается комплексная защита электронного документооборота. Обсуждаются методы и средства защиты от вредоносных программ, методы обнаружения и предотвращения вторжений в корпоративные информационные системы. Описываются функции межсетевых экранов и схемы защиты на базе межсетевых экранов. Рассматриваются методы и средства формирования виртуальных частных сетей, методы управления средствами обеспечения информационной безопасности. Описываются международные и отечественные стандарты информационной безопасности.

Рекомендуется в качестве учебного пособия по курсу «Информационная безопасность» для студентов факультета «Прикладные информационные технологии» МИЭТ, обучающихся по направлению «Информатика и вычислительная техника». Учебное пособие может быть полезно студентам, аспирантам и преподавателям вузов соответствующих специальностей.

ISBN 978-5-7256-0537-2

Учебное пособие

Шаньгин *Владимир Федорович*

Комплексная защита корпоративной информации

Технический редактор *Л.Г. Лосякова*. Корректор *Л.Г. Лосякова*. Компьютерная верстка *Е.А. Каменской*.

Подписано в печать с оригинал-макета 29.06.09. Формат 60x84 1/16. Печать офсетная.
Бумага офсетная. Гарнитура Times New Roman. Усл. печ. л. 23,43. Уч.-изд. л. 20,2.
Тираж 300 экз. Заказ 97.

Отпечатано в типографии ИПК МИЭТ.
124498, Москва, Зеленоград, проезд 4806, д. 5, МИЭТ.

Список сокращений

Access point - точка доступа - коммуникационный узел для пользователей или беспроводное устройство;
ACK (Acknowledgement) - подтверждение;
AES (Advanced Encryption Standard) - новый американский стандарт шифрования данных;
AH (Authentication Header) - аутентифицирующий заголовок в IPSec;
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;
DES (Data Encryption Standard) - бывший стандарт шифрования данных США; 3DES (Triple Data Encryption Standard) - алгоритм тройного шифрования, разновидность алгоритма DES;
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;
DSSS (Direct Sequence Spread Spectrum) - распределенный спектр с прямой последовательностью;
EAP (Extensible Authentication 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 электрике и электронике;
IEEE 802.11 - группа разработки стандартов в IEEE, цель которой - выпуск беспроводных стандартов локальных сетей LAN;
IKE (Internet Key Exchange) - протокол обмена ключами в Интернете;
IP (Internet Protocol) - интернет-протокол межсетевого обмена данными;
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 Керберос;
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 Ривестом (Ron Rivest) 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 - Адлеман;
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, используемый в США;
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 Интернет.

Предисловие

Познание начинается с удивления.

Аристотель

Стремительное развитие информационных технологий и быстрый рост 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, которые могут 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 волнуют 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.

Предлагаемое вниманию читателя учебное пособие посвящено систематическому изложению и анализу современных методов, средств и технологий комплексной защиты информации в корпоративных системах.

Содержание книги разбито на четыре логически связанных части.

Часть 1. Проблемы безопасности корпоративной информации.

Часть 2. Технологии защиты корпоративных данных.

Часть 3. Комплексная защита корпоративных информационных систем.

Часть 4. Управление информационной безопасностью.

Каждая из этих частей объединяет несколько глав, связанных общей темой. Книга содержит также предисловие и список литературы.

В связи с ограниченным объемом книги роль введения выполняет глава 1.

Часть 1 «Проблемы безопасности корпоративной информации» включает следующие главы:

- глава 1. Основные понятия и анализ угроз информационной безопасности;
- глава 2. Политики безопасности.

В главе 1 формулируются основные понятия и определения информационной безопасности и анализируются угрозы информационной безопасности в корпоративных информационных системах.

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

Часть 2 «Технологии защиты корпоративных данных» включает следующие главы:

- глава 3. Криптографическая защита информации;
- глава 4. Идентификация, аутентификация и управление доступом;
- глава 5. Защита электронного документооборота.

В главе 3 описываются такие криптографические методы защиты корпоративной информации, как симметричные и асимметричные криптосистемы шифрования, комбинированные криптосистемы, электронная цифровая подпись, функции хэширования и управление криптоключами. Подробно описывается инфраструктура управления открытыми ключами PKI (Public Key Infrastructure).

Глава 4 посвящена рассмотрению идентификации, аутентификации и авторизации пользователя. Описываются методы аутентификации, использующие многоразовые и одноразовые пароли, методы строгой аутентификации и биометрической аутентификации пользователей, управление доступом по схеме однократного входа Single Sign-On.

В главе 5 рассматриваются методы и средства защиты электронного документооборота. Формулируется концепция и особенности защиты электронного документооборота. Анализируются методы и средства защиты баз данных. Подробно описывается защита электронного почтового документооборота.

Рассматривается реализация отечественной системы защищенного электронного документооборота и управления взаимодействием DIRECTUM.

Часть 3 «Комплексная защита корпоративных информационных систем» объединяет следующие главы:

- глава 6. Принципы комплексной защиты информации КИС;
- глава 7. Защита от вредоносных программ;
- глава 8. Обнаружение и предотвращение вторжений;
- глава 9. Межсетевое экранирование;
- глава 10. Виртуальные защищенные сети VPN.

Глава 6 посвящена рассмотрению принципов комплексной защиты информации в корпоративных информационных системах. Анализируются особенности архитектуры КИС и структура системы защиты информации в КИС. Формулируется стратегия комплексного обеспечения информационной безопасности и описываются основные подсистемы информационной безопасности КИС.

В главе 7 описываются средства защиты от вредоносных программ. Приводится классификация вредоносных программ. Рассматриваются сигнатурный анализ и проактивные методы обнаружения вирусов и других вредоносных программ. Описывается защита корпоративной системы от вредоносных программ.

Глава 8 посвящена проблемам обнаружения и предотвращения вторжений. Рассматриваются методы обнаружения и предотвращения вторжений в корпоративные информационные системы, а также защита от распределенных атак.

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

Глава 10 представляет собой введение в защищенные виртуальные сети 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.

Часть 4 «Управление информационной безопасностью» объединяет следующие главы:

- глава 11. Управление средствами обеспечения информационной безопасности;
- глава 12. Стандарты информационной безопасности.

В главе 11 рассматриваются методы управления средствами защиты корпоративной информации. Формулируются 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. Приводится обзор современных систем управления информационной безопасностью.

Глава 12 посвящена описанию стандартов информационной безопасности. Рассматриваются основные международные стандарты информационной безопасности и, в частности, широко распространенный стандарт ISO 15408 «Общие критерии безопасности информационных технологий». Даются краткие описания популярных стандартов информационной безопасности для Интернета. Описываются отечественные стандарты безопасности информационных технологий.

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 (техническом университете).

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

Часть 1. ПРОБЛЕМЫ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

Новые информационные технологии активно внедряются во все сферы народного хозяйства. Появление 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.

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.

Хайям О. «Рубаи»

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.

1.1. Основные понятия защиты информации и информационной безопасности

Рассмотрим основные понятия защиты информации и информационной безопасности компьютерных систем с учетом определений стандарта ГОСТ Р 50922-96 (см. главу 12).

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 которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

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

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 защищаемой информации 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 информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих 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, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Под *информационной безопасностью* понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность 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, стихийные бедствия (землетрясение, ураган, пожар и т.п.).

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* - хранимые временно и постоянно, на магнитных носителях, печатные, 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, т.е. 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 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, т.е. 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 или 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, строка символов), идентифицирующую субъект. Эта информация является *идентификатором* субъекта системы (сети). Субъект, имеющий зарегистрированный идентификатор, является *законным (легитимным) 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* подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся 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 или используемые для защиты информации.

Комплекс средств защиты информации (КСЗИ) представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы (сети). КСЗИ 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 (КС) относятся к распределенным автоматизированным информационным системам, осуществляющим обработку информации. Обеспечение безопасности КС предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования КС, а также попыткам модификации, хищения, выведения из строя или разрушения ее компонентов, т.е. защиту всех компонентов КС - аппаратных средств, программного обеспечения, данных и персонала. Конкретный подход к проблеме обеспечения безопасности основан на разработанной для КС политике безопасности.

Политика безопасности - это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы от заданного множества угроз.

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

В настоящее время известен достаточно обширный перечень угроз информационной 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 информационной 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.

Классификация возможных угроз информационной безопасности ИС может быть проведена по ряду базовых признаков [1, 12].

1. *По природе возникновения* различают:

- *естественные угрозы*, вызванные воздействиями на ИС объективных физических процессов или стихийных природных явлений;
- *искусственные угрозы* безопасности ИС, вызванные деятельностью человека.

2. *По степени преднамеренности проявления* различают:

- *угрозы, вызванные ошибками или халатностью* персонала, например некомпетентное использование средств защиты, ввод ошибочных данных и т.п.;
- *угрозы преднамеренного действия*, например действия злоумышленников.

3. *По непосредственному источнику угроз*. Источниками угроз могут быть:

- *природная среда*, например стихийные бедствия, магнитные бури и пр.;
- *человек*, например вербовка путем подкупа персонала, разглашение конфиденциальных данных и т.п.;
- *санкционированные программно-аппаратные средства*, например удаление данных, отказ в работе операционной системы;
- несанкционированные программно-аппаратные средства, например заражение компьютера вирусами с деструктивными функциями.

4. *По положению источника угроз*. Источник угроз может быть расположен:

- *вне контролируемой зоны ИС*, например перехват данных, передаваемых по каналам связи, перехват электромагнитных, акустических и других излучений устройств;
- *в пределах контролируемой зоны ИС*, например применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т.п.;
- *непосредственно в ИС*, например некорректное использование ресурсов ИС.

5. *По степени зависимости от активности ИС*. Угрозы проявляются:

- *независимо от активности ИС*, например вскрытие шифров криптозащиты информации;
- *только в процессе обработки данных*, например угрозы выполнения и распространения программных вирусов.

6. *По степени воздействия на ИС* различают:

- *пассивные угрозы*, которые при реализации ничего не меняют в структуре и содержании ИС, например угроза копирования секретных данных;
- *активные угрозы*, которые при воздействии вносят изменения в структуру и содержание ИС, например внедрение «троянских коней» и вирусов.

7. *По этапам доступа пользователей или программ к ресурсам ИС* различают:

- угрозы, проявляющиеся *на этапе доступа к ресурсам ИС*, например угрозы несанкционированного доступа в ИС;
- угрозы, проявляющиеся *после разрешения доступа к ресурсам ИС*, например угрозы несанкционированного или некорректного использования ресурсов ИС.

8. *По способу доступа к ресурсам ИС* различают:

- угрозы *с использованием стандартного пути доступа* к ресурсам ИС, например незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя;
- угрозы *с использованием скрытого нестандартного пути доступа* к ресурсам ИС, например несанкционированный доступ к ресурсам ИС путем использования недокументированных возможностей операционных систем (ОС).

9. *По текущему месту расположения информации, хранимой и обрабатываемой в ИС*, различают:

- угрозы доступа к информации *на внешних запоминающих устройствах*, например несанкционированное копирование секретной информации с жесткого диска;
- угрозы доступа к информации *в оперативной памяти* например чтение остаточной информации из оперативной памяти, доступ к системной области оперативной памяти со стороны прикладных программ;
- угрозы доступа к информации, циркулирующей *в линиях связи*, например незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений, незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений;
- угрозы доступа к информации, отображаемой *на терминале или печатаемой на принтере*, например запись отображаемой информации на скрытую видеокамеру.

Как уже отмечалось, опасные воздействия на ИС подразделяют на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации ИС показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни и функционирования ИС.

Причинами *случайных воздействий* при эксплуатации ИС могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении (ПО);
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Ошибки в программном обеспечении являются распространенным видом компьютерных нарушений. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т.д. написано людьми, поэтому оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляют никакой опасности, некоторые же могут привести к серьезным последствиям, таким, как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (использование компьютера в качестве плацдарма для атаки и т.п.). Обычно подобные ошибки устраняются с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких пакетов является необходимым условием безопасности информации.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник и т.д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т.п.

Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить *гипотетическую модель потенциального нарушителя*:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

В частности, для банковских ИС можно выделить следующие преднамеренные угрозы:

- несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
- ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;

- несанкционированное копирование программ и данных;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных банковских документов;
- умышленное уничтожение информации;
- несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
- фальсификация сообщений, передаваемых по каналам связи;
- отказ от авторства сообщения, переданного по каналам связи;
- отказ от факта получения информации;
- навязывание ранее переданного сообщения;
- разрушение информации, вызванное вирусными воздействиями;
- разрушение архивной банковской информации, хранящейся на магнитных носителях;
- кража оборудования.

Наиболее распространенным и многообразным видом компьютерных нарушений является *несанкционированный доступ*. Суть НСД состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами ИС, так и специально созданными аппаратными и программными средствами.

Перечислим основные каналы несанкционированного доступа, через которые нарушитель может получить доступ к компонентам ИС и осуществить хищение, модификацию и/или разрушение информации:

- штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;
- технологические пульты управления;
- линии связи между аппаратными средствами ИС;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

Из всего разнообразия способов и приемов несанкционированного доступа остановимся на следующих распространенных и связанных между собой нарушениях:

- перехват паролей;
- «маскарад»;
- незаконное использование привилегий.

Перехват паролей осуществляется специально разработанными программами. При попытке законного пользователя войти в систему программа-перехватчик имитирует на экране дисплея ввод имени и пароля пользователя, которые сразу пересылаются владельцу программы-перехватчика, после чего на экран выводится сообщение об ошибке и управление возвращается операционной системе. Пользователь предполагает, что допустил ошибку при вводе пароля. Он повторяет ввод и получает доступ в систему. Владелец программы-перехватчика, получивший имя и пароль законного пользователя, может теперь использовать их в своих целях. Существуют и другие способы перехвата паролей.

«Маскарад» - это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями. Целью «маскарада» является приписывание каких-либо действий другому пользователю либо присвоение полномочий и привилегий другого пользователя. Примерами реализации «маскарада» являются:

- вход в систему под именем и паролем другого пользователя (этому «маскараду» предшествует перехват пароля);
- передача сообщений в сети от имени другого пользователя.

«Маскарад» особенно опасен в банковских системах электронных платежей, где неправильная идентификация клиента из-за «маскарада» злоумышленника может привести к большим убыткам законного клиента банка.

Незаконное использование привилегий - большинство систем защиты устанавливают определенные наборы привилегий для выполнения заданных функций. Каждый пользователь получает свой набор привилегий: обычные пользователи - минимальный, администраторы - максимальный. Несанкционированный захват привилегий, например, посредством «маскарада» приводит к возможности выполнения нарушителем определенных действий в обход системы защиты. Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

Вредоносные программы - к таким программам относятся «компьютерные вирусы», сетевые «черви», программа «троянский конь». Особенно уязвимы к этим программам рабочие станции конечных пользователей. Дадим краткую характеристику этих распространенных угроз безопасности ИС.

«Троянский конь» представляет собой программу, которая наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам. Аналогия такой программы с древнегреческим «троянским конем» вполне оправдана, так как в обоих случаях не вызывающая подозрений оболочка таит серьезную угрозу. Радикальный способ защиты от этой угрозы заключается в создании замкнутой среды исполнения программ, которые должны храниться и защищаться от несанкционированного доступа.

Компьютерный вирус представляет собой своеобразное явление, возникшее в процессе развития компьютерной и информационной техники. Суть этого явления состоит в том, что программы-вирусы обладают рядом свойств, присущих живым организмам, - они рождаются, размножаются и умирают. Термин «вирус» в применении к компьютерам предложил Фред Коэн из Университета Южной Калифорнии. Исторически первое определение, данное Ф. Коэном: «Компьютерный вирус - это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Компьютерные вирусы наносят ущерб системе за счет быстрого размножения и разрушения среды обитания.

Сетевой «червь» является разновидностью программы-вируса, которая распространяется по глобальной сети. Следует отметить, что «троянские кони», компьютерные вирусы и сетевые «черви» относятся к весьма опасным угрозам ИС.

Особенностью современных вредоносных программ является их ориентация на конкретное прикладное ПО, ставшее стандартом de facto для большинства пользователей, в первую очередь это Microsoft Internet Explorer и Microsoft Outlook. Массовое создание вирусов под продукты Microsoft объясняется не только низким уровнем безопасности и надежности программ, важную роль играет глобальное распространение этих продуктов. Авторы вредоносного программного обеспечения все активнее начинают исследовать «дыры» в популярных системах управления базами данных (СУБД), связующих ПО и корпоративные бизнес-приложения, построенные на базе этих систем.

Вредоносные программы постоянно эволюционируют, основной тенденцией их развития является полиморфизм. Сегодня уже довольно сложно провести границу между вирусом, «червем» и «троянским конем», они используют практически одни и те же механизмы, небольшая разница заключается лишь в степени этого использования. Устройство вредоносного программного обеспечения стало сегодня настолько унифицированными, что, например, отличить почтовый вирус от «червя» с деструктивными функциями практически невозможно. Даже в «троянских» программах появилась функция репликации (как одно из средств противодействия антивирусным средствам), так что при желании их вполне можно назвать вирусами (с механизмом распространения в виде маскировки под прикладные программы).

Для защиты от вредоносных программ необходимо применение ряда мер:

- исключить несанкционированный доступ к исполняемым файлам;
- тестировать приобретаемые программные средства;
- контролировать целостность исполняемых файлов и системных областей;
- создать замкнутую среду исполнения программ.

Борьба с вирусами, «червями» и «троянскими конями» ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и на уровне сети. По мере появления новых вирусов, «червей» и «троянских коней» нужно устанавливать новые базы данных антивирусных средств и приложений. Подробная классификация и характеристика вредоносных программ приводится в гл. 7, посвященной защите от вредоносных программ.

К непрограммным угрозам относятся спам, фишинг и фарминг. Распространенность этих угроз в последнее время значительно выросла.

Спам, объем которого сейчас превышает 80% от общего объема почтового трафика, может создавать угрозу доступности информации, блокируя почтовые серверы, либо использоваться для распространения вредоносного программного обеспечения.

Фишинг (phishing) является относительно новым видом интернет-мошенничества, цель которого - получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов, PIN-кодов и другой конфиденциальной информации, дающей доступ к деньгам пользователя. Фишинг использует не технические недостатки программного обеспечения, а легковерность пользователей Интернета. Сам термин «phishing», созвучный с «fishing» (рыбная ловля), расшифровывается как «password harvesting fishing» - выуживание пароля. Действительно, фишинг очень похож на рыбную ловлю. Злоумышленник закидывает в Интернет приманку и «вылавливает» всех «рыбок» - пользователей Интернета, которые клюнут на эту приманку.

Злоумышленником создается практически точная копия сайта выбранного банка (электронной платежной системы, аукциона и т.п.). Затем при помощи спам-технологии по электронной почте

рассылается письмо, составленное таким образом, чтобы быть максимально похожим на настоящее письмо от выбранного банка. При составлении письма используются логотипы банка, имена и фамилии реальных руководителей банка. В таком письме, как правило, сообщается о том, что из-за смены программного обеспечения в системе интернет-банкинга пользователю необходимо подтвердить или изменить свои учетные данные. В качестве причины для изменения данных могут быть названы выход из строя ПО банка или же нападение хакеров. Наличие правдоподобной легенды, побуждающей пользователя к необходимым действиям, - непременная составляющая успеха мошенников-фишеров. Во всех случаях цель таких писем одна - заставить пользователя нажать на приведенную ссылку, а затем ввести свои конфиденциальные данные (пароли, номера счетов, PIN-коды) на ложном сайте банка (электронной платежной системы, аукциона). Зайдя на ложный сайт, пользователь вводит в соответствующие строки свои конфиденциальные данные, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, в худшем - к электронному счету.

Технологии фишеров совершенствуются, применяются методы социальной инженерии. Клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свои конфиденциальные данные. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении.

В настоящее время мошенники часто используют «троянские» программы. Задача фишера в этом случае сильно упрощается - достаточно заставить пользователя перебраться на фишерский сайт и «подцепить» программу, которая самостоятельно разыщет на винчестере жертвы все, что нужно. Наравне с «троянскими» программами стали использоваться и кейлоггеры. На подставных сайтах на компьютеры жертв загружают шпионские утилиты, отслеживающие нажатия клавиш. При использовании такого подхода не обязательно находить выходы на клиентов конкретного банка или компании, а потому фишеры стали подделывать и сайты «общего назначения», такие, как новостные ленты и поисковые системы.

Успеху фишинг-афер способствует низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. В частности, около 5% пользователей не знают простого факта: банки не рассылают писем с просьбой подтвердить в онлайне номер своей кредитной карты и ее PIN-код.

Появилось сопряженное с фишингом понятие - фарминг.

Фарминг (Pharming) - это тоже вид мошенничества, ставящий целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNS цифровые адреса легитимных веб-сайтов на адреса поддельных, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид мошенничества еще опасней, так как заметить подделку практически невозможно.

По данным аналитиков (www.cnews.ru), ущерб, нанесенный фишерами мировой экономике, составил в 2004 году $44 млрд. По статистике Symantec, в середине 2004 года фильтры компании еженедельно блокировали до 9 млн писем с фишинговым контентом. К концу года за тот же период отсеивалось уже 33 млн.

Основной защитой от фишинга пока остаются спам-фильтры. К сожалению, программный инструментарий для защиты от фишинга обладает ограниченной эффективностью, поскольку злоумышленники эксплуатируют в первую очередь не бреши в ПО, а человеческую психологию. Активно разрабатываются технические средства безопасности, прежде всего плагины для популярных браузеров. Суть защиты заключается в блокировании сайтов, попавших в черные списки мошеннических ресурсов. Следующим шагом могут стать системы генерации одноразовых паролей для интернет-доступа к банковским счетам и аккаунтам в платежных системах, повсеместное распространение дополнительных уровней защиты за счет комбинации ввода пароля с использованием аппаратного USB-ключа.

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: *конфиденциальность, целостность и доступность информации*.

Другими словами, в соответствии с существующими подходами считают, что информационная безопасность ИС обеспечена в случае, если для информационных ресурсов в системе поддерживаются определенные уровни, а именно:

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

Соответственно для автоматизированных информационных систем рассматривают три основных вида угроз:

- *угрозы нарушения конфиденциальности*, направленные на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. В терминах компьютерной безопасности угроза нарушения

конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе или передаваемой от одной системы к другой;

· *угрозы нарушения целостности информации*, хранящейся в компьютерной системе или передаваемой по каналу связи, которые направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена умышленно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации - компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется полномочными лицами с обоснованной целью (например, таким изменением является периодическая коррекция некоторой базы данных);

- *угрозы нарушения работоспособности (отказ в обслуживании)*, направленные на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность ИС, либо блокируют доступ к некоторым ее ресурсам. 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.

Данные виды угроз можно считать первичными или непосредственными, поскольку реализация этих угроз ведет к непосредственному воздействию на защищаемую информацию.

Для современных информационных технологий подсистемы защиты являются неотъемлемой частью ИС обработки информации. Атакующая сторона должна преодолеть эту подсистему защиты, чтобы нарушить, например, конфиденциальность ИС. Однако нужно сознавать, что не существует абсолютно стойкой системы защиты, вопрос лишь во времени и средствах, требующихся на ее преодоление. Исходя из данных условий, рассмотрим следующую модель: защита информационной системы считается преодоленной, если в ходе исследования этой системы определены все ее уязвимости.

Преодоление защиты также представляет собой угрозу, поэтому для защищенных систем можно рассматривать четвертый вид угрозы - *угрозу раскрытия параметров ИС*, включающей в себя подсистему защиты. На практике любое проводимое мероприятие предваряется этапом разведки, в ходе которого определяются основные параметры системы, ее характеристики и т.п. Результатом этого этапа является уточнение поставленной задачи, а также выбор наиболее оптимального технического средства.

Угрозу раскрытия параметров ИС можно считать опосредованной угрозой. Последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность реализовать первичные или непосредственные угрозы, перечисленные выше.

При рассмотрении вопросов защиты ИС целесообразно использовать четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой ИС информации. Такая градация доступа поможет систематизировать как возможные угрозы, так и меры по их нейтрализации и парированию, т.е. поможет систематизировать весь спектр методов обеспечения защиты, относящихся к информационной безопасности. Это следующие уровни доступа:

- уровень носителей информации;
- уровень средств взаимодействия с носителем;
- уровень представления информации;
- уровень содержания информации.

Введение данных уровней обусловлено следующими соображениями.

Во-первых, информация для удобства манипулирования чаще всего фиксируется на некотором материальном носителе, которым может быть дискета или что-нибудь подобное.

Во-вторых, если способ представления информации таков, что она не может быть непосредственно воспринята человеком, возникает необходимость в преобразователях информации в доступный для человека способ представления. Например, для чтения информации с дискеты необходим компьютер, оборудованный дисководом соответствующего типа.

В-третьих, как уже было отмечено, информация может быть охарактеризована способом своего представления или тем, что еще называется языком в обиходном смысле. Язык символов, язык жестов и т.п. - все это способы представления информации.

В-четвертых, человеку должен быть доступен смысл представленной информации, ее семантика.

К основным направлениям реализации злоумышленником информационных *угроз* относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
- внедрение в технические средства ИС программных или технических механизмов, нарушающих предполагаемую структуру и функции ИС.

В табл.1.1 перечислены основные методы реализации угроз информационной безопасности.

Таблица 1.1

Основные методы реализации угроз информационной безопасности

Уровень доступа к информации в ИС	Методы реализации угроз информационной безопасности			
	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза отказа служб (отказа доступа к информации)
Уровень носителей информации	Определение типа и параметров носителей информации	Хищение (копирование) носителей информации	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Уровень средств взаимодействия с носителем	Получение информации о программно-аппаратной среде. Получение детальной информации о функциях, выполняемых ИС. Получение данных о применяемых системах защиты	Несанкционированный доступ к ресурсам ИС. Совершение пользователем несанкционированных действий. Несанкционирован-ное копирование программного обеспечения. Перехват данных, передаваемых по каналам связи	Внесение пользователем несанкционированных изменений в программы и данные. Установка и использование нештатного программного обеспечения. Заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонент ИС. Обход механизмов защиты ИС

Для достижения требуемого уровня информационной безопасности ИС необходимо обеспечить противодействие различным техническим угрозам и минимизировать возможное влияние человеческого фактора.

Рассмотрим *тенденции развития угроз для информационных технологий (ИТ-угроз)*. По мере развития и усложнения ИТ-инфраструктуры автоматически растет количество потенциальных ИТ-угроз и рисков. Кроме того, угрозы оказываются все более изощренными, поскольку хакеры, спамеры и иные злоумышленники активно берут на вооружение возможности, открывающиеся по мере развития информационных технологий.

Возрастание опасности внутренних ИТ-угроз - традиционно наиболее опасными считались внешние угрозы (в первую очередь вирусы), защите от которых уделялось особое внимание. Однако постепенно все больше возрастает опасность внутренних ИТ-угроз. В 2007 году инсайдерские угрозы впервые опередили вирусные, ранее неизменно находившиеся в первой строчке рейтинга как по числу инцидентов, так и по объему причиняемого ущерба.

В отчете «Trends in IT Security Threats», подготовленном Computer Economics, на первой позиции фигурируют угрозы со стороны инсайдеров (табл.1.2), опережающие по наносимому совокупному ущербу (финансовым убыткам и падению репутации компании) прочие виды угроз. Второе место досталось спаму - произошел заметный рост данного типа угроз. Угрозы от вредоносных программ занимают третье место в рейтинге, поскольку по-прежнему имеется немало организаций, где защита от подобных угроз пока реализована на недостаточном уровне.

На четвертом месте находится неавторизованный доступ со стороны внешних нарушителей, а на пятом - угроза физической потери носителя информации.

Таблица 1.2

Десятка наиболее опасных ИТ-угроз

Позиция в рейтинге	ИТ-угроза
1	Угроза инсайдеров
2	Спам
3	Угрозы от вредоносных программ (компьютерные вирусы, «черви», «троянцы», spyware-модули и adware-модули)
4	Неавторизованный доступ со стороны внешних нарушителей
5	Угроза физической потери носителя информации
6	Электронное мошенничество
7	Pharming-атаки
8	Phishing-атаки
9	Электронный вандализм и саботаж
10	DoS-атаки

Расширение спектра ИТ-угроз - сегодня все более серьезную угрозу для безопасности компаний представляют возрастающая мобильность пользователей (применение ноутбуков за пределами корпоративной сети стало практически повсеместным) и современные пользовательские ИТ-технологии (бесплатная почта, ICQ, чаты, блоги, Wi-Fi и пр.), все активнее проникающие в корпоративную сферу.

Мобильные устройства сотрудников и пользовательские ИТ-технологии (при всей своей полезности) представляют для компаний огромную опасность. Мобильные устройства вместе с находящейся на них корпоративной информацией нередко оказываются украденными или потерянными, причем часто находящаяся на них конфиденциальная информация никак не защищена. Кроме того, мобильные устройства и пользовательские технологии предоставляют множество способов скопировать конфиденциальную информацию, чем и пользуются инсайдеры.

Аналитики компании Gartner назвали мобильные устройства и пользовательские ИТ-технологии одной из наиболее существенных угроз корпоративной безопасности - и те и другие позволяют сотрудникам совершенно бесконтрольно копировать и распространять конфиденциальную информацию и увеличивают вероятность получить «вирус» или «троян». В связи с этим компаниям следует организовать просмотр всего http-трафика и peer-to-peer-трафика, блокировать подозрительные пакеты, контролировать использование мобильных носителей, ограничивать и контролировать удаленный доступ (в том числе беспроводный) и т.д.

1.3. Способы обеспечения безопасности информационных систем

Существуют два подхода к проблеме обеспечения безопасности информационных систем: фрагментарный и комплексный [11, 14].

Фрагментарный подход направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т.п. Достоинством такого подхода является высокая избирательность к конкретной угрозе. Существенным недостатком данного подхода является отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов ИС только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты.

Комплексный подход ориентирован на создание защищенной среды обработки информации в ИС, объединяющей в единый комплекс разнородные меры противодействия угрозам. Организация защищенной среды обработки информации позволяет гарантировать определенный уровень безопасности ИС, что является несомненным достоинством комплексного подхода. К недостаткам этого подхода относятся: ограничения на свободу действий пользователей ИС, чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

Комплексный подход применяют для защиты (корпоративных информационных систем (КИС) крупных организаций или небольших ИС, выполняющих ответственные задачи или обрабатывающих особо важную информацию. Нарушение безопасности информации в КИС крупных организаций может нанести огромный материальный ущерб как самим организациям, так и их клиентам. Поэтому такие организации вынуждены уделять особое внимание гарантиям безопасности и реализовывать комплексную защиту. Комплексного подхода придерживаются большинство государственных и крупных коммерческих предприятий и учреждений. Этот подход нашел свое отражение в различных стандартах.

Комплексный подход к проблеме обеспечения безопасности основан на разработанной для конкретной ИС политике безопасности. Политика безопасности регламентирует эффективную работу средств защиты ИС. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Надежная система безопасности сети не может быть создана без эффективной политики сетевой безопасности.

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательно-нормативного (законы, стандарты, нормативные акты и т.п.);
- административно-организационного (действия общего характера, предпринимаемые руководством организации, и конкретные меры безопасности, имеющие дело с людьми);
- программно-технического (конкретные технические меры).

Меры законодательно-нормативного уровня очень важны для обеспечения информационной безопасности. К этому уровню можно отнести весь комплекс мер, направленных на создание и поддержание в обществе и на предприятии негативного отношения к нарушениям и нарушителям информационной безопасности.

Меры административно-организационного уровня - администрация организации должна сознавать необходимость поддержания режима безопасности и выделения на эти цели соответствующих ресурсов. Основой мер защиты административно-организационного уровня является политика безопасности и комплекс организационных мер. Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов организации.

К комплексу организационных мер относятся следующие меры безопасности:

- управление персоналом;

- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Для поддержания режима информационной безопасности особенно важны меры программно-технического уровня, поскольку основная угроза компьютерным системам исходит от них самих: сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т.п.

Меры и средства программно-технического уровня - в рамках современных информационных систем должны быть доступны, по крайней мере, следующие средства и механизмы безопасности:

- средства криптографии;
- механизмы идентификации и аутентификации;
- средства контроля доступа к рабочим местам;
- средства обнаружения и предотвращения атак;
- средства защиты от вредоносных программ;
- средства протоколирования и аудита;
- средства централизованного управления защитой информации.

Необходимость применения стандартов - информационные системы компаний почти всегда построены на основе программных и аппаратных продуктов различных производителей, поскольку нет ни одной компании-разработчика, которая предоставила бы потребителю полный перечень средств для построения современной ИС. Чтобы обеспечить в разнородной ИС надежную защиту информации, требуются специалисты высокой квалификации, которые будут отвечать за безопасность каждого компонента ИС: правильно их настраивать, постоянно отслеживать происходящие изменения, контролировать работу пользователей.

Очевидно, что чем разнороднее информационная система, тем сложнее обеспечить ее безопасность. Изобилие в корпоративных сетях и системах разнообразных средств защиты, а также растущий спрос на доступ к корпоративным данным со стороны сотрудников, партнеров и заказчиков приводят к созданию сложной среды защиты, трудной для управления.

Для большинства гетерогенных сред важно обеспечить согласованное взаимодействие с продуктами других производителей. Интероперабельность продуктов защиты является важным требованием для большинства корпоративных информационных систем. Поэтому вполне очевидна потребность в применении единого набора стандартов поставщиками средств защиты, компаниями - системными интеграторами и организациями, выступающими в качестве заказчиков систем безопасности для своих корпоративных сетей и систем.

Стандарты образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности, и определяют критерии, которым должно следовать управление безопасностью. Стандарты являются необходимой базой, обеспечивающей совместимость продуктов разных производителей, что чрезвычайно важно при создании систем сетевой безопасности в гетерогенных средах. Международные и отечественные стандарты информационной безопасности рассматриваются в гл. 12.

Комплексный подход к решению проблемы обеспечения безопасности, рациональное сочетании законодательных, административно-организационных и программно-технических мер и обязательное следование промышленным, национальным и международным стандартам являются тем фундаментом, на котором строится вся система защиты корпоративных информационных систем.

Вопросы для самоконтроля

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Объясните понятия идентификации, аутентификации и авторизации пользователя. Как они взаимосвязаны?
4. Укажите отличия санкционированного доступа от несанкционированного доступа к информации.
5. Сформулируйте определение политики безопасности.
6. Сформулируйте особенности избирательной и полномочной политики безопасности.
7. Объясните понятие «угроза безопасности ИС».
8. Укажите основные признаки классификации возможных угроз безопасности ИС.
9. Каковы основные виды угроз безопасности ИС по цели и степени воздействия?
10. Дайте краткую характеристику угроз безопасности, обозначаемых терминами: «троянский конь», «вирус», «червь»?
11. Перечислите и дайте краткую характеристику основных методов реализации угроз информационной безопасности.
12. Объясните суть комплексного подхода к обеспечению информационной безопасности ИС.

Глава 2. Политика информационной безопасности

Если начинают с неправильного,
то мало надежды на правильное завершение.
Конфуций

Под *политикой безопасности* организации понимают совокупность управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Вообще политика безопасности определяется используемой компьютерной средой и отражает специфические потребности организации.

Обычно 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. По мере роста компьютерной системы и интеграции ее в глобальную сеть необходимо обеспечить отсутствие в системе слабых мест, поскольку все усилия по защите информации могут быть обесценены лишь одной оплошностью.

Можно построить политику безопасности, которая будет устанавливать, кто имеет доступ к конкретным активам и приложениям, какие роли и обязанности будут иметь конкретные лица, а также предусмотреть процедуры безопасности, которые четко предписывают, как должны выполняться конкретные задачи безопасности. Индивидуальные особенности работы сотрудника могут потребовать доступа к информации, которая не должна быть доступна другим работникам. Например, менеджер по персоналу может иметь доступ к частной информации любого сотрудника, в то время как специалист по отчетности может иметь доступ только к финансовым данным этих сотрудников. А рядовой сотрудник будет иметь доступ только к своей собственной персональной информации.

Политика безопасности определяет позицию организации по рациональному использованию компьютеров и сети, а также процедуры по предотвращению и реагированию на инциденты безопасности. В большой корпоративной системе может применяться широкий диапазон разных политик - от бизнес-политик до специфичных правил доступа к наборам данных. Эти политики полностью определяются конкретными потребностями организации.

2.1. Основные понятия политики безопасности

Политика безопасности определяет стратегию управления в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую считает целесообразным выделить руководство.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Для того чтобы познакомиться с основными понятиями политик безопасности, рассмотрим в качестве конкретного примера гипотетическую ИС, принадлежащую некоторой организации, и ассоциированную с ней политику безопасности [1].

Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого рядом более конкретных документов специализированных политик и процедур безопасности.

Высокоуровневая политика безопасности должна периодически пересматриваться, чтобы гарантировать, что она учитывает текущие потребности организации. Этот документ составляют таким образом, чтобы политика была относительно независимой от конкретных технологий. В таком случае этот документ политики не потребуется изменять слишком часто. Политика безопасности обычно оформляется в виде документа, включающего такие разделы, как описание проблемы, область применения, позиция организации, распределение ролей и обязанностей, санкции и др.

Описание проблемы - информация, циркулирующая в рамках ИС, является критически важной. ИС позволяет пользователям совместно использовать программы и данные, что увеличивает угрозу безопасности. Поэтому каждый из компьютеров, входящих в ИС, нуждается в более сильной защите. Эти повышенные меры безопасности и являются темой данного документа. Документ преследует следующие цели - продемонстрировать сотрудникам организации важность защиты сетевой среды, описать их роль в

обеспечении безопасности, а также распределить конкретные обязанности по защите информации, циркулирующей в ИС.

Область применения - в сферу действия данной политики попадают все аппаратные, программные и информационные ресурсы, входящие в ИС предприятия. Политика ориентирована также на людей, работающих с ИС, в том числе на пользователей, субподрядчиков и поставщиков.

Позиция организации - целью организации является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности. Более частными целями являются:

- обеспечение уровня безопасности, соответствующего нормативным документам;
- следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности);
- обеспечение безопасности в каждой функциональной области ИС;
- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
- обеспечение анализа регистрационной информации;
- предоставление пользователям достаточной информации для сознательного поддержания режима безопасности;
- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы ИС;
- обеспечение соответствия с имеющимися законами и общеорганизационной политикой безопасности.

Распределение ролей и обязанностей - за реализацию сформулированных выше целей отвечают соответствующие должностные лица и пользователи ИС. *Руководители подразделений* отвечают за доведение положений политики безопасности до пользователей и за контакты с ними. *Администраторы ИС* обеспечивают непрерывное функционирование ИС и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности. *Администраторы сервисов* отвечают за конкретные сервисы и, в частности, за то, чтобы защита была построена в соответствии с общей политикой безопасности. *Пользователи* обязаны работать с ИС в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.

Ниже приведены более подробные сведения о ролях и обязанностях должностных лиц и пользователей ИС.

Санкции - нарушение политики безопасности может подвергнуть ИС и циркулирующую в ней информацию недопустимому риску. Случаи нарушения безопасности со стороны персонала должны оперативно рассматриваться руководством для принятия дисциплинарных мер вплоть до увольнения.

Дополнительная информация - конкретным группам исполнителей могут потребоваться для ознакомления какие-то дополнительные документы, в частности документы специализированных политик и процедур безопасности, а также другие руководящие указания. Необходимость в дополнительных документах политик безопасности в значительной степени зависит от размеров и сложности организации. Для достаточно большой организации могут потребоваться в дополнение к базовой политике специализированные политики безопасности. Организации меньшего размера нуждаются только в некотором подмножестве специализированных политик. Многие из этих документов поддержки могут быть довольно краткими - объемом в одну-две страницы.

С практической точки зрения политики безопасности можно разделить на три уровня: верхний, средний и нижний [1, 14].

Верхний уровень политики безопасности определяет решения, затрагивающие организацию в целом. Эти решения носят весьма общий характер и исходят, как правило, от руководства организации.

Такие решения могут включать в себя следующие элементы:

- формулировку целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- формирование или пересмотр комплексной программы обеспечения информационной безопасности, определение ответственных лиц за продвижение программы;
- обеспечение материальной базы для соблюдения законов и правил;
- формулировку управленческих решений по вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Политика безопасности верхнего уровня формулирует цели организации в области информационной безопасности в терминах целостности, доступности и конфиденциальности. На верхний уровень выносится управление ресурсами безопасности и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. В-третьих,

необходимо обеспечить исполнительскую дисциплину персонала с помощью системы поощрений и наказаний.

Средний уровень политики безопасности определяет решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией. Примеры таких вопросов - отношение к доступу в Интернет (проблема сочетания свободы получения информации с защитой от внешних угроз), использование домашних компьютеров и т.д.

Политика безопасности среднего уровня должна определять для каждого аспекта информационной безопасности следующие моменты:

- *описание аспекта* - позиция организации может быть сформулирована в достаточно общем виде как набор целей, которые преследует организация в данном аспекте;
- *область применения* - следует специфицировать, где, когда, как, по отношению к кому и чему применяется данная политика безопасности;
- *роли и обязанности* - документ должен содержать информацию о должностных лицах, отвечающих за проведение политики безопасности в жизнь;
- *санкции* - политика должна содержать общее описание запрещенных действий и наказаний за них;
- *точки контакта* - должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит должностное лицо.

Нижний уровень политики безопасности относится к конкретным сервисам. Эта политика включает в себя два аспекта - цели и правила их достижения, поэтому ее трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть более детальной.

Приведем несколько примеров вопросов**,** на которые следует дать ответ при следовании политике безопасности нижнего уровня:

- Кто имеет право доступа к объектам, поддерживаемым сервисом?
- При каких условиях можно читать и модифицировать данные?
- Как организован удаленный доступ к сервису?

В общем случае цели должны связывать между собой объекты сервиса и осмысленные действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем детальнее правила, чем более четко и формально они изложены, тем проще поддержать их выполнение программно-техническими мерами. Обычно наиболее формально задаются права доступа к объектам.

Кратко сформулируем обязанности каждой категории персонала.

Руководители подразделений отвечают за доведение положений политики безопасности до пользователей.

Администраторы ИС обеспечивают непрерывное функционирование ИС и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.

Администраторы сервисов отвечают за конкретные сервисы и, в частности, за то, чтобы защита была построена в соответствии с общей политикой безопасности.

Пользователи обязаны работать с ИС в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.

Главной целью мер, предпринимаемых на управленческом уровне, является формирование программы работ в области информационной безопасности и обеспечение ее выполнения путем выделения необходимых ресурсов и осуществления регулярного контроля состояния дел. Основой этой программы является многоуровневая политика безопасности, отражающая комплексный подход организации к защите своих ресурсов и информационных активов.

2.2. Структура политики безопасности организации

Для большинства организаций политика безопасности абсолютно необходима. Политика безопасности определяет отношение организации к обеспечению безопасности и необходимые действия организации по защите своих ресурсов и активов. На основе политики безопасности устанавливаются необходимые средства и процедуры безопасности, а также определяются роли и ответственность сотрудников организации в обеспечении безопасности.

Обычно политика безопасности организации включает следующие компоненты:

- базовую политику безопасности;
- процедуры безопасности;
- специализированные политики безопасности (рис.2.1).

Основные положения политики безопасности организации описываются в следующих документах:

- обзор политики безопасности;

- описание базовой политики безопасности;
- руководство по архитектуре безопасности.

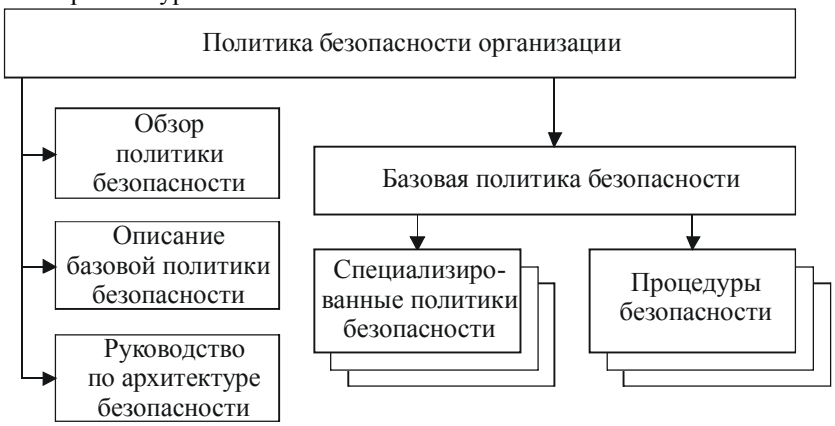

Рис.2.1. Структура политики безопасности организации

Главным компонентом политики безопасности организации является базовая политика безопасности [1].

2.2.1. Базовая политика безопасности

Базовая политика безопасности устанавливает, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать. В описании базовой политики безопасности определяются разрешенные и запрещенные действия, а также указываются необходимые средства управления в рамках реализуемой архитектуры безопасности. С базовой политикой безопасности согласовываются специализированные политики и процедуры безопасности.

Нисходящий подход, реализуемый базовой политикой безопасности, дает возможность постепенно и последовательно выполнять работу по созданию системы безопасности, не пытаясь сразу выполнить ее целиком. Базовая политика позволяет в любое время ознакомиться с политикой безопасности в полном объеме и выяснить текущее состояние безопасности в организации.

Обзор политики безопасности раскрывает цель политики безопасности, описывает структуру политики безопасности, подробно излагает, кто и за что отвечает, устанавливает процедуры и предполагаемые временные рамки для внесения изменений. В зависимости от масштаба организации политика безопасности может содержать больше или меньше разделов.

Руководство по архитектуре безопасности описывает реализацию механизмов безопасности в компонентах архитектуры, используемых в сети организации.

Как отмечалось выше, структура и состав политики безопасности зависит от размера и целей компании. Обычно базовая политика безопасности организации поддерживается набором специализированных политик и процедур безопасности.

2.2.2. Специализированные политики безопасности

Потенциально существуют десятки специализированных политик, которые могут применяться большинством организаций среднего и большого размера. Некоторые политики предназначаются для каждой организации, другие политики специфичны для определенных компьютерных окружений.

С учетом особенностей применения специализированные политики безопасности можно разделить на две группы:

- политики, затрагивающие значительное число пользователей;
- политики, связанные с конкретными техническими областями.

К специализированным политикам, затрагивающим значительное число пользователей, относятся:

- политика допустимого использования;
- политика удаленного доступа к ресурсам сети;
- политика защиты информации;
- политика защиты паролей и др.

К специализированным политикам, связанным с конкретными техническими областями, относятся:

- политика конфигурации межсетевых экранов;
- политика по шифрованию и управлению криптоключами;
- политика безопасности виртуальных защищенных сетей VPN;
- политика по оборудованию беспроводной сети и др.

Рассмотрим подробнее некоторые из ключевых специализированных политик.

Политика допустимого использования. Базовая политика безопасности обычно связана с рядом политик допустимого использования. Целью политики допустимого использования является установление стандартных норм безопасного использования компьютерного оборудования и сервисов в компании, а также соответствующих мер безопасности сотрудников с целью защиты корпоративных ресурсов и собственной информации. Неправильное использование компьютерного оборудования и сервисов подвергает компанию рискам, включая вирусные атаки, компрометацию сетевых систем и сервисов. Конкретный тип и количество политик допустимого использования зависят от результатов анализа требований бизнеса, оценки рисков и корпоративной культуры в организации.

Политика допустимого использования применяется к сотрудникам, консультантам, временным служащим и другим работникам в компании, включая сотрудников сторонних организаций. Политика допустимого использования предназначается в основном для конечных пользователей. Эта политика указывает пользователям, какие действия разрешены, а какие запрещены.

Политика допустимого использования должна установить:

- ответственность пользователей за защиту любой информации, используемой и/или хранимой их компьютерами;
- могут ли пользователи читать и копировать файлы, которые не являются их собственными, но доступны им;
- уровень допустимого использования для электронной почты и Web-доступа.

Существует много видов политики допустимого использования. В частности, могут быть политики допустимого использования для компьютеров, передачи данных, коммуникаций электронной почты, портативных персональных компьютеров, Web-доступа и др.

Для образовательных и государственных учреждений политика допустимого использования, по существу, просто обязательна. Без зафиксированной в соответствующем документе политики допустимого использования штатные сотрудники управления и поддержки сети не имеют формальных оснований для принятия санкций к своему или стороннему сотруднику, который допустил грубое нарушение правил безопасной работы на компьютере или в сети.

Для политики допустимого использования не существует специального формата. В этой политике должно быть указано имя сервиса, системы или подсистемы (например, политика использования компьютера, электронной почты, компактных компьютеров и паролей) и описано в самых четких терминах разрешенное и запрещенное поведение. В этой политике должны быть также подробно описаны последствия нарушения ее правил и санкции, налагаемые на нарушителя.

Разработка политики допустимого использования выполняется квалифицированными специалистами по соответствующему сервису, системе или подсистеме под контролем комиссии (команды), которой поручена разработка политики безопасности организации.

Политика удаленного доступа. Целью политики удаленного доступа является установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании. Эти стандартные нормы призваны минимизировать ущерб компании из-за возможного неавторизованного использования ресурсов компании. К такому ущербу относятся утрата интеллектуальной собственности компании, потеря конфиденциальных данных, искажение имиджа компании, повреждения критических внутренних систем компании и т.д.

Эта политика касается всех сотрудников, поставщиков и агентов компании при использовании ими для удаленного соединения с сетью компании компьютеров или рабочих станций, являющихся собственностью компании или находящихся в личной собственности.

Политика удаленного доступа:

- намечает и определяет допустимые методы удаленного соединения с внутренней сетью;
- существенна в большой организации, где сети территориально распределены и простираются до домов;
- должна охватывать по возможности все распространенные методы удаленного доступа к внутренним ресурсам.

Политика удаленного доступа должна определить:

- какие методы разрешаются для удаленного доступа;
- ограничения на данные, к которым можно получить удаленный доступ;
- кто может иметь удаленный доступ.

Защищенный удаленный доступ должен быть строго контролируемым. Применяемая процедура контроля должна гарантировать, что доступ к надлежащей информации или сервисам получат только прошедшие проверку люди. Сотрудник компании не должен передавать свой логин и пароль никогда и никому, включая членов своей семьи. Управление удаленным доступом не должно быть настолько сложным, чтобы это приводило к возникновению ошибок.

Контроль доступа целесообразно выполнять с помощью одноразовой парольной аутентификации или с помощью открытых/секретных ключей (см. гл. 3 и 4).

Сотрудники компании с правами удаленного доступа должны обеспечить, чтобы принадлежащие им или компании персональный компьютер или рабочая станция, которые удаленно подсоединены к корпоративной сети компании, не были связаны в это же время с какой-либо другой сетью, за исключением персональных сетей, находящихся под полным контролем пользователя.

Сотрудники компании с правами удаленного доступа к корпоративной сети компании должны обеспечить, чтобы их соединение удаленного доступа имело такие же характеристики безопасности, как обычное локальное соединение с компанией.

Все хосты, которые подключены к внутренним сетям компании с помощью технологий удаленного доступа, должны использовать самое современное антивирусное обеспечение, это требование относится и к персональным компьютерам компании.

Любой сотрудник компании, уличенный в нарушении данной политики, может быть подвергнут дисциплинарному взысканию вплоть до увольнения с работы.

2.2.3. Процедуры безопасности

Процедуры безопасности важны не менее, чем политики. Процедуры безопасности являются необходимым и важным дополнением к политикам безопасности. Политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты. Процедуры безопасности определяют, как защитить ресурсы и каковы механизмы исполнения политики, т.е. как реализовывать политики безопасности.

По существу, процедуры безопасности представляют собой пошаговые инструкции для выполнения оперативных задач. Часто процедура является тем инструментом, с помощью которого политика преобразуется в реальное действие. Например, политика паролей формулирует правила конструирования паролей, правила о том, как защитить ваш пароль и как часто заменять пароли. Процедура управления паролями описывает процесс создания новых паролей, распределения их, а также процесс гарантированной смены паролей на критичных устройствах.

Процедуры безопасности детально определяют действия, которые нужно предпринять при реагировании на конкретные события. Процедуры безопасности обеспечивают быстрое реагирование в критической ситуации. Процедуры помогают устранить проблему единой точки отказа в работе, если, например, во время кризиса работник неожиданно покидает рабочее место или оказывается недоступен.

Многие процедуры, связанные с безопасностью, должны быть стандартными средствами в любом подразделении. В качестве примеров можно указать процедуры для резервного копирования и внесистемного хранения защищенных копий, а также процедуры для вывода пользователя из активного состояния и/или архивирования логина и пароля пользователя, применяемые сразу, как только данный пользователь увольняется из организации.

Рассмотрим несколько важных процедур безопасности, которые необходимы почти каждой организации.

Процедура реагирования на события. Данная процедура является необходимым средством безопасности для большинства организаций. Организация особенно уязвима, когда обнаруживается вторжение в ее сеть или когда она сталкивается со стихийным бедствием. Нетрудно представить, что произойдет в последующие минуты и часы, если интеллектуальная собственность компании составляет миллионы или миллиарды долларов.

Процедуру реагирования на события иногда называют *процедурой обработки событий* или *процедурой реагирования на инциденты*. Практически невозможно указать отклики на все события нарушений безопасности, но нужно стремиться охватить основные типы нарушений, которые могут произойти.

Некоторые примеры событий нарушений безопасности: сканирование портов сети, атака типа отказ в обслуживании, компрометация хоста, несанкционированный доступ и др.

Данная процедура определяет:

- обязанности членов команды реагирования;
- какую информацию регистрировать и прослеживать;
- как обрабатывать исследование отклонений от нормы и атаки вторжения;
- кого уведомлять и когда;
- кто может выпускать в свет информацию и какова процедура выпуска информации;
- как должен выполняться последующий анализ и кто будет в этом участвовать.

В команду реагирования могут быть включены должностные лица компании, менеджер маркетинга (для связи с прессой), системный и сетевой администраторы и представитель соответствующих правоохранительных органов. Процедура должна указать, когда и в каком порядке они вызываются.

Процедура управления конфигурацией. Процедура управления конфигурацией обычно определяется на корпоративном уровне или уровне подразделения. Эта процедура должна определить процесс документирования и запроса изменений конфигурации на всех уровнях принятия решений. В принципе, должна существовать центральная группа, которая рассматривает все запросы на изменения конфигурации и принимает необходимые решения.

Процедура управления конфигурацией определяет:

- кто имеет полномочия выполнить изменения конфигурации аппаратного и программного обеспечения;
- как тестируется и инсталлируется новое аппаратное и программное обеспечение;
- как документируются изменения в аппаратном и программном обеспечении;

- кто должен быть проинформирован, когда случаются изменения в аппаратном и программном обеспечении.

Процесс управления конфигурацией важен по нескольким причинам:

- документирует сделанные изменения и обеспечивает возможность аудита;
- документирует возможный простой системы;
- дает способ координировать изменения так, чтобы одно изменение не помешало другому изменению.

2.3. Разработка политики безопасности организации

Разработка политики безопасности является ключевым этапом построения защищенной информационной системы или сети. Следует отметить, что составление политики безопасности или политик является только началом осуществления общей программы обеспечения безопасности организации. Детальная программа обеспечения безопасности необходима для создания эффективной системы безопасности организации на основе разработанной политики безопасности.

Основными этапами программы обеспечения безопасности являются следующие:

- определение ценности технологических и информационных активов организации;
- оценка рисков этих активов (сначала путем идентификации тех угроз, для которых каждый актив является целевым объектом, а затем оценкой вероятности того, что эти угрозы будут реализованы на практике);
- установление уровня безопасности, определяющего защиту каждого актива, т.е. мер безопасности, которые можно считать рентабельными для применения;
- формирование на базе предыдущих этапов политики безопасности организации;
- привлечение необходимых финансовых ресурсов для реализации политики безопасности, приобретение и установка требуемых средств безопасности;
- проведение разъяснительных мероприятий и обучения персонала для поддержки сотрудниками и руководством требуемых мер безопасности;
- регулярный контроль пошаговой реализации плана безопасности с целью выявления текущих проблем, учета изменения внешнего окружения и внесение необходимых изменений в состав персонала.

Опыт показал, что в целом организации получают существенную выгоду от реализации хорошо разработанной методологии решения указанных выше задач.

Первыми шагами по разработке политики безопасности являются следующие:

- создание команды по разработке политики;
- принятие решения об области действия и целях политики;
- принятие решения об особенностях разрабатываемой политики;
- определение лица или органа для работы в качестве официального интерпретатора политики.

Ко всем разрабатываемым политикам безопасности целесообразно применять унифицированный процесс проектирования с единообразными требованиями к политикам.

Одним из первых шагов является *создание команды по разработке политики безопасности организации*. Иногда эту команду называют группой, комиссией или комитетом. Команда создается руководством организации, которое должно осознавать важность информационной безопасности и полностью реализовать свою позитивную роль в успешной разработке, принятии и внедрении этой политики.

В состав команды следует включать квалифицированных специалистов, хорошо разбирающихся в требованиях бизнеса, информационных технологиях и безопасности, юриста и члена руководства, который сможет проводить в жизнь эту политику безопасности. К работе этой команды должны быть также привлечены администраторы безопасности и системные администраторы, представитель от сообщества пользователей.

Размер команды по разработке политики зависит от масштаба и области действия политики. Крупномасштабные политики могут потребовать команды из 5 - 10 человек, в то время как политики небольшого масштаба могут потребовать только одного или двух человек.

Как только создана такая команда, ее первым шагом является *анализ требований бизнеса*. Члены команды с различными позициями и точками зрения должны проанализировать требования бизнеса к использованию компьютерных и сетевых сервисов. Когда мнения некоторых членов этой команды не совпадают, столкновения их интересов и пересечения разных отраслей знания при обсуждении требований бизнеса позволяют получить более полную и объективную картину, чем при обычном опросе людей, работающих в области маркетинга, продаж или разработки [1].

На этом этапе анализируются и решаются вопросы типа: Какие компьютерные и сетевые сервисы требуются для бизнеса, и как эти требования могут быть удовлетворены при условии обеспечения безопасности? Сколько сотрудников зависят от доступа в Интернет, использования e-mail и доступности интранет-сервисов? Зависят ли компьютерные и сетевые сервисы от удаленного доступа к внутренней сети? Имеются ли требования по доступу к Web? Требуются ли клиентам данные тех-

нической поддержки через Интернет? При анализе каждого сервиса следует обязательно спрашивать, имеется ли требование бизнеса на этот сервис. Это - самый важный вопрос.

После анализа и систематизации требований бизнеса команда по разработке политики безопасности переходит к анализу и оценке рисков. Использование информационных систем и сетей связано с определенной совокупностью рисков.

Анализ рисков является важнейшим этапом формирования политики безопасности (рис.2.2).

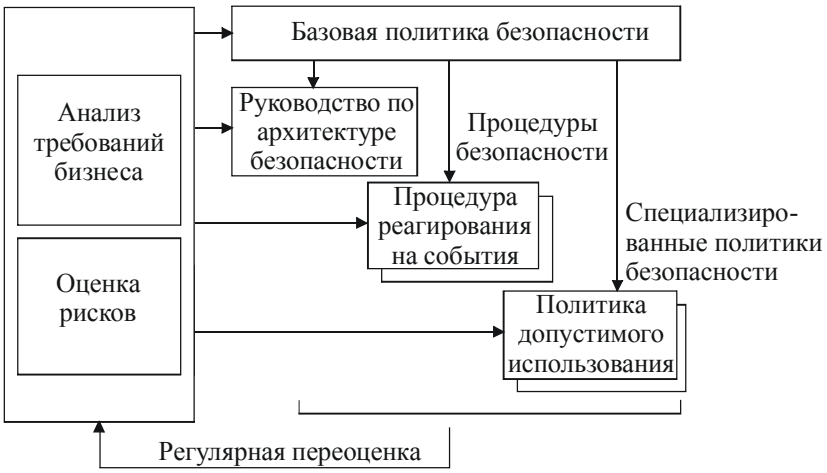

Рис.2.2. Схема разработки политики безопасности

Иногда этот этап называют также *анализом уязвимостей* или *оценкой угроз*. Хотя эти термины имеют несколько различающиеся толкования, конечные результаты сходны.

На этапе анализа рисков осуществляются следующие действия:

- идентификация и оценка стоимости технологических и информационных активов;
- анализ тех угроз, для которых данный актив является целевым объектом;
- оценка вероятности того, что угроза будет реализована на практике;
- оценка рисков этих активов [1].

Оценка риска выявляет как наиболее ценные, так и наиболее уязвимые активы, она позволяет точно установить, на какие проблемы нужно обратить особое внимание. Отчет об оценке рисков является ценным инструментом при формировании политики сетевой безопасности.

После оценки рисков активов можно переходить к *установлению уровня безопасности*, определяющего защиту каждого актива, т.е. *мер безопасности*, которые можно считать рентабельными для применения.

В принципе, *стоимость защиты конкретного актива не должна превышать стоимости самого актива*. Необходимо составить подробный перечень всех активов, который включает такие материальные объекты, как серверы и рабочие станции, и такие нематериальные объекты, как данные и программное обеспечение. Должны быть идентифицированы директории, которые содержат конфиденциальные файлы или файлы целевого назначения. После идентификации этих активов должно быть проведено определение стоимости замены каждого актива с целью назначения приоритетов в перечне активов.

Для контроля эффективности деятельности в области безопасности и для учета изменений обстановки необходима *регулярная переоценка рисков*.

После проведения описанной выше работы можно переходить к непосредственному составлению политики безопасности. В политике безопасности организации должны быть определены используемые стандарты, правила и процессы безопасности.

Стандарты указывают, каким критериям должно следовать управление безопасностью. *Правила* подробно описывают принципы и способы управления безопасностью. *Процессы* должны осуществлять точную реализацию правил в соответствии с принятыми стандартами.

Кроме того, политика безопасности должна определить значимые для безопасности *роли* и указать *ответственности этих ролей*. Роли устанавливаются во время формулирования процессов безопасности.

Руководство по архитектуре безопасности детально определяет контрмеры против угроз, раскрытых при оценке рисков. Это руководство описывает компоненты архитектуры безопасности ИС, рекомендует конкретные продукты безопасности и дает инструкции, как развернуть и управлять ими. В частности, это руководство может содержать рекомендации, где следует поставить межсетевые экраны, когда использовать шифрование, где разместить Web-серверы и как организовать управление коммуникациями с бизнес-партнерами и заказчиками. Руководство по архитектуре безопасности определяет также гарантии безопасности, аудит и средства контроля.

Вопросы для самоконтроля

1. Объясните понятие «политика безопасности организации».
2. Какие разделы должна содержать документально оформленная политика безопасности?
3. Какие проблемы решает верхний уровень политики безопасности?
4. Какие задачи решает средний уровень политики безопасности?
5. Каковы особенности нижнего уровня политики безопасности?
6. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
7. Опишите структуру политики безопасности организации.
8. Что представляют собой специализированные политики безопасности?
9. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.
10. Что представляют собой процедуры безопасности?
11. Приведите несколько примеров процедур безопасности с описанием их особенностей.
12. Сформулируйте основные этапы разработки политики безопасности организации.

Часть 2. ТЕХНОЛОГИИ ЗАЩИТЫ КОРПОРАТИВНЫХ ДАННЫХ

Безопасность корпоративных данных означает их конфиденциальность, целостность и подлинность. Критерии безопасности корпоративных данных могут быть определены следующим образом.

Конфиденциальность данных предполагает их доступность только для тех лиц, которые имеют на это соответствующие полномочия. Под *обеспечением конфиденциальности* информации понимается создание таких условий, при которых понять содержание передаваемых данных может только законный получатель, которому данная информация предназначена.

Целостность информации предполагает ее неизменность в процессе передачи от отправителя к получателю. Под *обеспечением целостности* информации понимается достижение идентичности отправляемых и принимаемых данных.

Подлинность информации предполагает соответствие этой информации ее явному описанию и содержанию, в частности соответствие действительным характеристикам указанных отправителя, времени отправления и содержания. *Обеспечение подлинности* информации, реализуемое на основе аутентификации, состоит в достоверном установлении отправителя, а также защите информации от изменения при ее передаче от отправителя к получателю. Своевременно обнаруженное нарушение подлинности и целостности полученного сообщения позволяет предотвратить отрицательные последствия, связанные с дальнейшим использованием такого искаженного сообщения.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования/расшифрования.

Глава 3. Криптографическая защита информации

Нет ничего тайного,
что не сделалось бы явным.
Евангелие от Луки. 8:17

Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Исторически криптография (в переводе с греческого этот термин означает «тайнопись») зародилась как способ скрытой передачи сообщений. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей. Такие преобразования обеспечивают решение трех главных проблем защиты данных: обеспечение конфиденциальности, целостности и подлинности передаваемых или сохраняемых данных.

3.1. Основные понятия криптографической защиты информации

Для обеспечения безопасности данных необходимо поддерживать три основные функции:

- защиту конфиденциальности передаваемых или хранимых в памяти данных;
- подтверждение целостности и подлинности данных;
- аутентификацию пользователей при входе в систему и установлении соединения.

Для реализации указанных функций используются криптографические технологии шифрования и цифровой подписи, а также средства аутентификации.

Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т.п.

Целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования.

Аутентификация разрешает устанавливать соединения только между легитимными пользователями и предотвращает доступ к средствам сети нежелательных лиц. Абонентам, доказавшим свою легитимность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

Основой большинства криптографических средств защиты информации является *шифрование данных*.

Под *шифром* понимают совокупность процедур и правил криптографических преобразований, используемых для зашифрования и расшифрования информации по ключу шифрования. Под

зашифрованием информации понимается процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют *расшифрованием* (дешифрованием).

Обобщенная схема криптосистемы шифрования показана на рис.3.1.

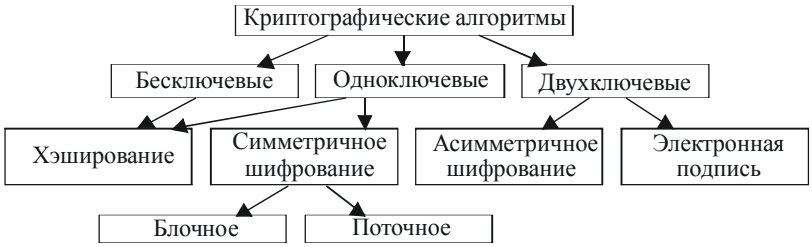

Рис.3.2. Классификация криптоалгоритмов защиты информации

Исходный текст передаваемого сообщения (или хранимой информации) *M* зашифровывается с помощью криптографического преобразования E_{k1} с получением в результате *шифртекста C*:

$$C = E_{k1}(M),$$

где *k*1 - параметр функции *E*, называемый ключом шифрования.

Шифртекст *C*, называемый еще *криптограммой*, содержит исходную информацию *M* в полном объеме, однако последовательность знаков в нем внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования *k*1.

Ключ шифрования является тем элементом, с помощью которого можно варьировать результат криптографического преобразования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (или владельцами).

Обратное преобразование информации выглядит следующим образом:

$$M' = D_{k2}(C).$$

Функция* D *является обратной к функции* E *и производит расшифрование шифртекста. Она также имеет дополнительный параметр в виде ключа* k2. *Ключ расшифрования* k2 *должен однозначно соответствовать ключу* k1, *в этом случае полученное в результате расшифрования сообщение* M' *будет эквивалентно* M. *При отсутствии верного ключа* k2 *получить исходное сообщение* M' = M *с помощью функции* D *невозможно.

Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования. Соответственно различают два основных класса криптосистем:

- симметричные;
- асимметричные.

Известны несколько классификаций криптографических алгоритмов, например показанная на рис.3.2 [7].

Охарактеризуем кратко основные типы криптоалгоритмов.

Хэширование - это метод криптозащиты, представляющий собой контрольное преобразование информации: из данных неограниченного размера путем выполнения криптографических преобразований вычисляется хэш-значение фиксированной длины, однозначно соответствующее исходным данным. Хэширование может выполняться как с использованием некоторого секретного ключа, так и без него. Такое криптографическое контрольное суммирование широко используется в различных методах защиты информации, в частности, для подтверждения целостности данных, если использование электронной подписи невозможно (например, из-за большой ресурсоемкости) или избыточно. Кроме того, данный метод применяется в схемах электронной подписи («подписывается» обычно хэш-значение данных, а не все данные целиком), а также в схемах аутентификации пользователей (при проверке, действительно ли пользователь является тем, за кого себя выдает).

Симметричное шифрование использует один и тот же ключ как для зашифрования, так и для расшифрования информации. Фактически оба ключа (зашифрования и расшифрования) могут и различаться, но если в каком-либо криптоалгоритме их легко вычислить один из другого в обе стороны, такой алгоритм однозначно относится к симметричному шифрованию.

Симметричное шифрование подразделяется на два вида: блочное и поточное, хотя стоит сразу отметить, что в некоторых классификациях они не разделяются и считается, что поточное шифрование - это шифрование блоков единичной длины.

Блочное шифрование характеризуется тем, что информация предварительно разбивается на блоки фиксированной длины (например, 64 или 128 бит). При этом в различных криптоалгоритмах или даже в разных режимах работы одного и того же алгоритма блоки могут шифроваться как независимо друг от друга, так и «со сцеплением» - когда результат шифрования текущего блока данных зависит от значения предыдущего блока или от результата шифрования предыдущего блока.

Поточное шифрование применяется прежде всего тогда, когда информацию невозможно разбить на блоки. Например, есть некий поток данных, каждый символ которых требуется зашифровать и отправить, не дожидаясь остальных данных, достаточных для формирования блока. Алгоритмы поточного шифрования шифруют данные побитно или посимвольно.

Асимметричное шифрование характеризуется применением двух типов ключей: открытого - для зашифрования информации и секретного - для ее расшифрования. Секретный и открытый ключи связаны между собой достаточно сложным соотношением. Главное в этом соотношении - легкость вычисления открытого ключа из секретного и невозможность (за ограниченное время при реальных ресурсах) вычисления секретного ключа из открытого при достаточно большой размерности операндов.

Электронная цифровая подпись (ЭЦП) используется для подтверждения целостности и авторства данных. Как и в случае асимметричного шифрования, в данном методе применяются двухключевые алгоритмы с таким же простым вычислением открытого ключа из секретного и практической невозможностью обратного вычисления. Однако назначение ключей ЭЦП совершенно иное. Секретный ключ применяется для вычисления ЭЦП, открытый ключ необходим для ее проверки. При соблюдении правил безопасного хранения секретного ключа никто, кроме его владельца, не в состоянии вычислить верную ЭЦП какого-либо электронного документа.

3.2. Симметричные криптосистемы шифрования

Исторически первыми появились симметричные криптографические системы. В симметричной криптосистеме шифрования используется один и тот же ключ для зашифрования и расшифрования информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение. Соответственно, с целью предотвращения несанкционированного раскрытия зашифрованной информации все ключи шифрования в симметричных криптосистемах должны держаться в секрете. Именно поэтому симметричные криптосистемы называют криптосистемами с секретным ключом - ключ шифрования должен быть доступен только тем, кому предназначено сообщение. Симметричные криптосистемы называют еще одноключевыми криптографическими системами или криптосистемами с закрытым ключом. Схема симметричной криптосистемы шифрования показана на рис.3.3.

Данные криптосистемы характеризуются наиболее высокой скоростью шифрования и с их помощью обеспечивается как конфиденциальность и подлинность, так и целостность передаваемой информации.

Конфиденциальность передачи информации с помощью симметричной криптосистемы зависит от надежности шифра и обеспечения конфиденциальности ключа шифрования. Обычно ключ шифрования представляет собой файл или массив данных и хранится на персональном ключевом носителе, например дискете или смарт-карте; обязательно принятие мер, обеспечивающих недоступность персонального ключевого носителя кому-либо, кроме его владельца.

Подлинность обеспечивается за счет того, что без предварительного расшифрования практически невозможно осуществить смысловую модификацию и подлог криптографически закрытого сообщения. Фальшивое сообщение не может быть правильно зашифровано без знания секретного ключа.

Целостность данных обеспечивается присоединением к передаваемым данным специального кода (имитовставки), вырабатываемой по секретному ключу. Имитовставка является разновидностью контрольной суммы, т.е. некоторой эталонной характеристикой сообщения, по которой осуществляется проверка целостности последнего. Алгоритм формирования имитовставки должен обеспечивать ее зависимость по некоторому сложному криптографическому закону от каждого бита сообщения. Проверка целостности сообщения выполняется получателем сообщения путем выработки по секретному ключу имитовставки, соответствующей полученному сообщению, и ее сравнения с полученным значением имитовставки. При совпадении делается вывод о том, что информация не была модифицирована на пути от отправителя к получателю.

Симметричное шифрование идеально подходит для шифрования информации «для себя», например, с целью предотвратить несанкционированный доступ к ней в отсутствие владельца. Это может быть как архивное шифрование выбранных файлов, так и прозрачное (автоматическое) шифрование целых логических или физических дисков.

Имея высокую скорость шифрования, одноключевые криптосистемы позволяют решать многие важные задачи защиты информации. Однако автономное использование симметричных криптосистем в компьютерных сетях порождает проблему распределения ключей шифрования между пользователями.

Перед началом обмена зашифрованными данными необходимо обменяться секретными ключами со всеми адресатами. Передача секретного ключа симметричной криптосистемы не может быть осуществлена по общедоступным каналам связи, секретный ключ надо передавать отправителю и получателю по защищенному каналу.

Характерной особенностью симметричных криптоалгоритмов является то, что в ходе своей работы они производят преобразование блока входной информации фиксированной длины и получают результирующий блок того же объема, но недоступный для прочтения сторонним лицам, не владеющим ключом. Схему работы симметричного блочного шифра можно описать функциями

$$C = E_K(M) \text{ и } M = D_K(C),$$

где* M - *исходный (открытый) блок данных;* C - *зашифрованный блок данных.

Ключ *K* является параметром симметричного блочного криптоалгоритма и представляет собой блок двоичной информации фиксированного размера. Исходный *M* и зашифрованный *C* блоки данных также имеют фиксированную разрядность, равную между собой, но не обязательно равную длине ключа *K*.

Блочные шифры являются той основой, на которой реализованы практически все симметричные криптосистемы. Симметричные криптосистемы позволяют кодировать и декодировать файлы произвольной длины. Практически все алгоритмы используют для преобразований определенный набор обратимых математических преобразований.

Методика создания цепочек из зашифрованных блочными алгоритмами байтов позволяет шифровать ими пакеты информации неограниченной длины. Отсутствие статистической корреляции между битами выходного потока блочного шифра используется для вычисления контрольных сумм пакетов данных и в хэшировании паролей. На сегодняшний день разработано достаточно много стойких блочных шифров.

Криптоалгоритм считается идеально стойким, если для прочтения зашифрованного блока данных необходим перебор всех возможных ключей до тех пор, пока расшифрованное сообщение не окажется осмысленным. В общем случае стойкость блочного шифра зависит только от длины ключа и возрастает экспоненциально с ее ростом.

Для получения стойких блочных шифров используют два общих принципа: рассеивание и перемешивание.

Рассеивание представляет собой распространение влияния одного знака открытого текста на много знаков шифртекста, что позволяет скрыть статистические свойства открытого текста.

Перемешивание предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов. Однако шифр должен не только затруднять раскрытие, но и обеспечивать легкость шифрования и расшифрования при известном пользователю секретном ключе.

Распространенным способом достижения эффектов рассеивания и перемешивания является использование составного шифра, т.е. такого шифра, который может быть реализован в виде некоторой последовательности простых шифров, каждый из которых вносит свой вклад в значительное суммарное рассеивание и перемешивание. В составных шифрах в качестве простых шифров чаще всего используются простые перестановки и подстановки. При перестановке просто перемешивают символы открытого текста, причем конкретный вид перемешивания определяется секретным ключом. При подстановке каждый символ открытого текста заменяют другим символом из того же алфавита, а конкретный вид подстановки также определяется секретным ключом. Следует заметить, что в современном блочном шифре блоки открытого текста и шифртекста представляют собой двоичные последовательности обычно длиной 64 или 128 бит. При длине 64 бита каждый блок может принимать 2^{64} значений. Поэтому подстановки выполняются в очень большом алфавите, содержащем до $2^{64} \approx 10^{19}$ «символов».

При многократном чередовании простых перестановок и подстановок, управляемых достаточно длинным секретным ключом, можно получить стойкий шифр с хорошим рассеиванием и перемешиванием.

Все действия, производимые блочным криптоалгоритмом над данными, основаны на том факте, что преобразуемый блок может быть представлен в виде целого неотрицательного числа из диапазона, соответствующего его разрядности. Например, 32-битный блок данных можно интерпретировать как число из диапазона 0...4 294 967 295. Кроме того, блок, разрядность которого представляет собой «степень двойки», можно трактовать как сцепление нескольких независимых неотрицательных чисел из меньшего диапазона (указанный выше 32-битный блок можно также представить в виде сцепления двух независимых 16-битных чисел из диапазона 0...65535 или в виде сцепления четырех независимых 8-битных чисел из диапазона 0...255). Над этими числами блочный криптоалгоритм производит по определенной схеме следующие действия.

Математические функции

Сложение	$X' = X + V$.
Исключающее ИЛИ	$X' = X$ XOR V.

***Умножение по модулю 2*N+1**	**X' = (X*V) mod (2N + 1).**
***Умножение по модулю 2*N**	**X' = (X*V) mod (2N).**

Битовые сдвиги

Арифметический сдвиг влево	*X′* = *X* SHL *V*.
Арифметический сдвиг вправо	*X′* = *X* SHR *V*.
Циклический сдвиг влево	*X′* = X ROL *V*.
Циклический сдвиг вправо	*X′* = X ROR *V*.

Табличные подстановки

S-box (англ. substitute)	*X′* = Table[*X*, *V*].

В качестве параметра *V* для любого из этих преобразований может использоваться:

· ***фиксированное число (например,* X' = X + *125);***

· ***число, получаемое из ключа (например,* X' = X + F*(K));***

• число, получаемое из независимой части блока (например, *X*2′ = *X*2 + *F*(*X*1)).

Последний вариант используется в схеме, называемой сетью Фейстеля (по имени ее создателя).

Последовательность выполняемых над блоком операций, комбинации перечисленных выше вариантов *V* и сами функции *F* и составляют отличительные особенности конкретного симметричного блочного криптоалгоритма.

Характерным признаком блочных алгоритмов является многократное и косвенное использование материала ключа. Это определяется в первую очередь требованием невозможности обратного декодирования в отношении ключа при известных исходном и зашифрованном текстах. Для решения этой задачи в приведенных выше преобразованиях чаще всего используется не само значение ключа или его части, а некоторая, иногда необратимая, функция от материала ключа. Более того, в подобных преобразованиях один и тот же блок или элемент ключа используется многократно. Это позволяет при выполнении условия обратимости функции относительно величины *X* сделать функцию необратимой относительно ключа *K* [16].

3.2.1. Алгоритмы шифрования DES и 3DES

Алгоритм шифрования данных DES (Data Encryption Standard) был опубликован в 1977 году. Блочный симметричный алгоритм DES остается пока распространенным алгоритмом, используемым в системах защиты коммерческой информации.

Алгоритм DES построен в соответствии с методологией сети Фейстеля и состоит из чередующейся последовательности перестановок и подстановок. Алгоритм DES осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (остальные 8 бит - проверочные биты для контроля на четность). Обобщенная схема процесса шифрования в блочном алгоритме DES показана на рис.3.4.

Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах (раундах) шифрования и, наконец, в конечной перестановке битов.

Расшифрование в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности.

Основные достоинства алгоритма DES:

• используется только один ключ длиной 56 бит;

· ***относительная простота алгоритма обеспечивает высокую скорость обработки;***

• зашифровав сообщение с помощью одного пакета программ, для расшифровки можно использовать любой другой пакет программ, соответствующий алгоритму DES;

• криптостойкость алгоритма вполне достаточна для обеспечения информационной безопасности большинства коммерческих приложений.

Современная микропроцессорная техника позволяет уже сегодня за достаточно приемлемое время взламывать симметричные блочные шифры с длиной ключа 40 бит. Для такого взламывания используется метод полного перебора - тотального опробования всех возможных значений ключа (метод «грубой силы»).

До недавнего времени блочный алгоритм DES, имеющий ключ с эффективной длиной 56 бит, считался относительно безопасным алгоритмом шифрования. Он многократно подвергался тщательному криптоанализу в течение 20 лет, и самым практичным способом его взламывания является метод перебора всех возможных значений ключа. Ключ шифра DES имеет 2^{56} возможных значений.

Появились дешевые чипы, способные перебирать сотни миллионов ключей в секунду (ASIC-чипы и др.). Поэтому вполне актуальны оценки криптостойкости шифра DES, включающие ориентировочные расчеты времени и материальных средств, которые необходимо затратить на взламывание этого шифра методом полного перебора всех возможных значений ключа с использованием как стандартных компьютеров, так и

специализированных криптоаналитических аппаратных средств. В табл.3.1 приведены результаты анализа трудоемкости взламывания криптоалгоритма DES [11].

Таблица 3.1

Сравнительный анализ трудоемкости взлома криптоалгоритма DES

Возникает естественный вопрос: нельзя ли использовать DES в качестве модуля для создания другого алгоритма с более длинным ключом?

Существует много способов *комбинирования блочных алгоритмов* для получения новых алгоритмов. Одним из таких способов комбинирования является многократное шифрование, т.е. использование блочного алгоритма несколько раз с разными ключами для шифрования одного и того же блока открытого текста.

У. Тачмен предложил шифровать блок открытого текста P три раза с помощью двух ключей $K1$ и $K2$ (рис.3.5) [11].

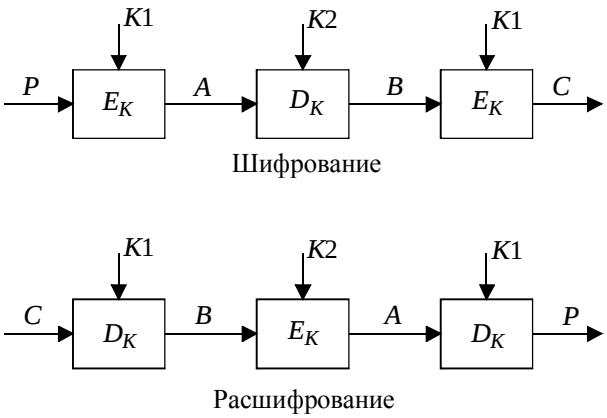

Рис.3.5. Схемы трехкратного применения блочного алгоритма симметричного шифрования с двумя различными ключами

Процедура шифрования:

$$C = E_{K1}(D_{K2}(E_{K1}(P))),$$

т.е. блок открытого текста P сначала шифруется ключом $K1$, затем расшифровывается ключом $K2$ и окончательно зашифровывается ключом $K1$.

Этот режим иногда называют режимом EDE (encrypt-decrypt-encrypt). Введение в данную схему операции расшифрования D_{K2} позволяет обеспечить совместимость этой схемы со схемой однократного использования блочного алгоритма DES. Если в схеме трехкратного использования DES выбрать все ключи одинаковыми, то эта схема превращается в схему однократного использования DES. Процедура расшифрования выполняется в обратном порядке:

$$P = D_{K1}(E_{K2}(D_{K1}(C))),$$

т.е. блок шифртекста C сначала расшифровывается ключом $K1$, затем зашифровывается ключом $K2$ и окончательно расшифровывается ключом $K1$.

Если исходный блочный алгоритм имеет n-битовый ключ, то схема трехкратного шифрования имеет $2n$-битовый ключ. Чередование ключей $K1$ и $K2$ позволяет предотвратить криптоаналитическую атаку «встреча посредине». Данная схема приводится в стандартах X9.17 и ISO 8732 в качестве средства улучшения характеристик алгоритма DES.

При трехкратном шифровании можно применить три различных ключа. При этом возрастает общая длина результирующего ключа. Процедуры шифрования и расшифрования описываются выражениями:

$$C = E_{K3}(D_{K2}(E_{K1}(P))),$$

$$P = D_{K1}(E_{K2}(D_{K3}(C))).$$

Трехключевой вариант имеет еще большую стойкость. Алгоритм 3DES (Triple DES - тройной DES) используется в ситуациях, когда надежность алгоритма DES считается недостаточной. Чаще всего используется вариант шифрования на трех ключах: открытый текст шифруется на первом ключе, полученный шифртекст - на втором ключе и, наконец, данные, полученные после второго шага,

шифруются на третьем ключе. Все три ключа выбираются независимо друг от друга. Этот криптоалгоритм достаточно стоек ко всем атакам. Применяется также каскадный вариант 3DES. Это - стандартный тройной DES, к которому добавлен такой механизм обратной связи, как CBC, OFB или CFB.

Сегодня все шире используются два современных криптостойких алгоритма шифрования: отечественный стандарт шифрования ГОСТ 28147-89 и новый криптостандарт США - AES (Advanced Encryption Standard).

3.2.2. Стандарт шифрования ГОСТ 28147-89

Этот алгоритм криптографического преобразования данных предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не налагает ограничений на степень секретности защищаемой информации. Алгоритм шифрования данных, определяемый ГОСТ 28147-89, представляет собой 64-битовый блочный алгоритм с 256-битовым ключом.

Данные, подлежащие зашифрованию, разбивают на 64-разрядные блоки. Эти блоки разбиваются на два субблока *N*1 и *N*2 по 32 бит (рис.3.6).

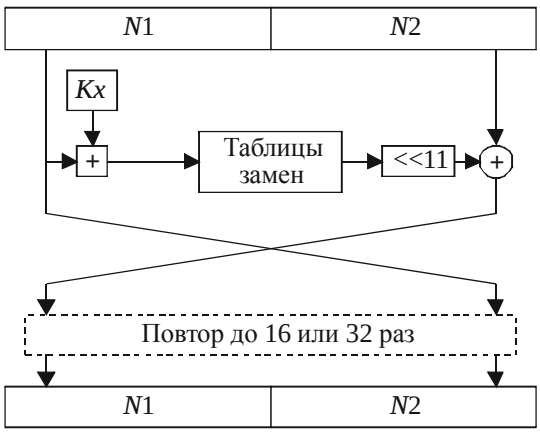

Рис.3.6. Схема алгоритма ГОСТ 28147-89

Субблок *N*1 обрабатывается определенным образом, после чего его значение складывается со значением субблока *N*2 (сложение выполняется по модулю 2, т.е. применяется логическая операция XOR - исключающее ИЛИ), а затем субблоки меняются местами. Данное преобразование выполняется определенное число раз (раундов): 16 или 32 в зависимости от режима работы алгоритма. В каждом раунде выполняются две операции.

Первая операция - наложение ключа. Содержимое субблока *N*1 складывается по модулю 2^{32} с 32-битовой частью ключа *Kx*. Полный ключ шифрования представляется в виде конкатенации 32-битовых подключей: *K*0, *K*1, *K*2, *K*3, *K*4, *K*5, *K*6, *K*7. В процессе шифрования используется один из этих подключей - в зависимости от номера раунда и режима работы алгоритма.

Вторая операция - табличная замена. После наложения ключа субблок *N*1 разбивается на 8 частей по 4 бит, значение каждой из которых заменяется в соответствии с таблицей замены для данной части субблока. Затем выполняется побитовый циклический сдвиг субблока влево на 11 бит.

Блок подстановки *S*-box (Substitution box) часто используется в современных алгоритмах шифрования, поэтому стоит пояснить, как организуется операция «*табличная замена*».

Блок подстановки *S*-box состоит из восьми узлов замены (*S*-блоков замены) S_1, S_2,..., S_8 с памятью 64 бит каждый. Поступающий на блок подстановки *S* 32-битовый вектор разбивают на восемь последовательно идущих 4-битовых векторов, каждый из которых преобразуется в 4-битовый вектор соответствующим узлом замены. Каждый узел замены можно представить в виде таблицы-перестановки шестнадцати 4-битовых двоичных чисел в диапазоне 0000…1111. Входной вектор указывает адрес строки в таблице, а число в этой строке является выходным вектором. Затем 4-битовые выходные векторы последовательно объединяют в 32-битовый вектор. Узлы замены (таблицы-перестановки) представляют собой ключевые элементы, которые являются общими для сети ЭВМ и редко изменяются. Эти узлы замены должны сохраняться в секрете.

Алгоритм, определяемый ГОСТ 28147-89, предусматривает четыре режима работы: простой замены, гаммирования, гаммирования с обратной связью и генерации имитовставок. В них используется одно и то же описанное выше шифрующее преобразование, но, поскольку назначение режимов различно, осуществляется это преобразование в каждом из них по-разному.

В режиме *простой замены* для зашифрования каждого 64-битового блока информации выполняются 32 описанных выше раунда. При этом 32-битовые подключи используются в следующей последовательности:

*K*0, *K*1, *K*2, *K*3, *K*4, *K*5, *K*6, *K*7, *K*0, *K*1 и т.д. - в раундах с 1-го по 24-й;

*K*7, *K*6, *K*5, *K*4, *K*3, *K*2, *K*1, *K*0 - в раундах с 25-го по 32-й.

Расшифрование в данном режиме проводится точно так же, но с несколько другой последовательностью применения подключей:

*K*0, *K*1, *K*2, *K*3, *K*4, *K*5, *K*6, *K*7 - в раундах с 1-го по 8-й;

*K*7, *K*6, *K*5, *K*4, *K*3, *K*2, *K*1, *K*0, *K*7, *K*6 и т.д. - в раундах с 9-го по 32-й.

Все блоки шифруются независимо друг от друга, т.е. результат зашифрования каждого блока зависит только от его содержимого (соответствующего блока исходного текста). При наличии нескольких одинаковых блоков исходного (открытого) текста соответствующие им блоки шифртекста тоже будут одинаковы, что дает дополнительную полезную информацию для пытающегося вскрыть шифр криптоаналитика. Поэтому данный режим применяется в основном для шифрования самих ключей шифрования (очень часто реализуются многоключевые схемы, в которых по ряду соображений ключи шифруются друг на друге). Для шифрования собственно информации предназначены два других режима работы - гаммирования и гаммирования с обратной связью.

В *режиме гаммирования* каждый блок открытого текста побитно складывается по модулю 2 с блоком гаммы шифра размером 64 бит. *Гамма шифра* - это специальная последовательность, которая получается в результате определенных операций с регистрами *N*1 и *N*2 (рис.3.7):

1) в регистры N1 и N2 записывается их начальное заполнение - 64-битовая величина, называемая синхропосылкой;

2) выполняется зашифрование содержимого регистров *N*1 и *N*2 (в данном случае - синхропосылки) в режиме простой замены;

3) содержимое регистра *N*1 складывается по модулю $(2^{32} - 1)$ с константой $C1 = 2^{24} + 2^{16} + 2^8 + 2^4$, а результат сложения записывается в регистр *N*1;

4) содержимое регистра *N*2 складывается по модулю 232 с константой $C2 = 2^{24} + 2^{16} + 2^8 + 1$, а результат сложения записывается в регистр *N*2;

5) содержимое регистров *N*1 и *N*2 подается на выход в качестве 64-битового блока гаммы шифра (в данном случае *N*1 и *N*2 образуют первый блок гаммы).

Если необходим следующий блок гаммы (т.е. необходимо продолжить зашифрование или расшифрование), выполняется возврат к операции 2.

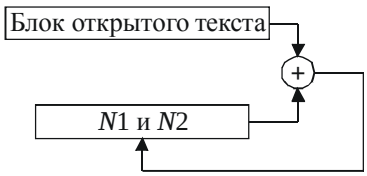

Рис.3.7. Выработка гаммы шифра в режиме гаммирования с обратной связью

Для расшифрования гамма вырабатывается аналогичным образом, а затем к битам зашифрованного текста и гаммы снова применяется операция XOR. Поскольку эта операция обратима, в случае правильно выработанной гаммы получается исходный текст (табл.3.2).

Таблица 3.2

Зашифрование и расшифрование в режиме гаммирования

	Операция	Результат
Исходный текст		100100
Гамма	XOR	111000
Шифртекст	=	011100
Гамма	XOR	111000
Исходный текст	=	100100

Для выработки нужной для расшифровки гаммы шифра у пользователя, расшифровывающего криптограмму, должен быть тот же ключ и то же значение синхропосылки, которые применялись при зашифровывании информации. В противном случае получить исходный текст из зашифрованного не удастся.

В большинстве реализаций алгоритма ГОСТ 28147-89 синхропосылка не секретна, однако есть системы, где синхропосылка - такой же секретный элемент, как и ключ шифрования. Для таких систем эффективная длина ключа алгоритма (256 бит) увеличивается еще на 64 бит секретной синхропосылки, которую также можно рассматривать как ключевой элемент.

В *режиме гаммирования с обратной связью* для заполнения регистров $N1$ и $N2$, начиная со 2-го блока, используется не предыдущий блок гаммы, а результат зашифрования предыдущего блока открытого текста (см. рис.3.7). Первый же блок в данном режиме генерируется полностью аналогично предыдущему.

Рассматривая режим *генерации имитовставок*, следует определить понятие предмета генерации. Имитовставка - это криптографическая контрольная сумма, вычисляемая с использованием ключа шифрования и предназначенная для проверки целостности сообщений. При генерации имитовставки выполняются следующие операции: первый 64-битовый блок массива информации, для которого вычисляется имитовставка, записывается в регистры $N1$ и $N2$ и зашифровывается в сокращенном режиме простой замены (выполняются первые 16 раундов из 32). Полученный результат суммируется по модулю 2 со следующим блоком информации с сохранением результата в $N1$ и $N2$.

Цикл повторяется до последнего блока информации. Получившееся в результате этих преобразований 64-битовое содержимое регистров $N1$ и $N2$ или его часть и называется имитовставкой. Размер имитовставки выбирается, исходя из требуемой достоверности сообщений: при длине имитовставки r бит вероятность, что изменение сообщения останется незамеченным, равна 2^{-r}.

Чаще всего используется 32-битовая имитовставка, т.е. половина содержимого регистров. Этого достаточно, поскольку, как любая контрольная сумма, имитовставка предназначена прежде всего для защиты от случайных искажений информации. Для защиты же от преднамеренной модификации данных применяются другие криптографические методы - в первую очередь электронная цифровая подпись.

При обмене информацией имитовставка служит своего рода дополнительным средством контроля. Она вычисляется для открытого текста при зашифровании какой-либо информации и посылается вместе с шифртекстом. После расшифрования вычисляется новое значение имитовставки, которое сравнивается с присланной. Если значения не совпадают, значит шифртекст был искажен при передаче или при расшифровании использовались неверные ключи. Особенно полезна имитовставка для проверки правильности расшифрования ключевой информации при использовании многоключевых схем.

Алгоритм ГОСТ 28147-89 считается очень стойким - в настоящее время для его раскрытия не предложено более эффективных методов, чем упомянутый выше метод «грубой силы». Его высокая стойкость достигается в первую очередь за счет большой длины ключа - 256 бит. При использовании секретной синхропосылки эффективная длина ключа увеличивается до 320 бит, а засекречивание таблицы замен прибавляет дополнительные биты. Кроме того, криптостойкость зависит от количества раундов преобразований, которых по ГОСТ 28147-89 должно быть 32 (полный эффект рассеивания входных данных достигается уже после 8 раундов).

3.2.3. Американский стандарт шифрования AES

В 1997 году Американский институт стандартизации NIST (National Institute of Standards & Technology) объявил конкурс на новый стандарт симметричного криптоалгоритма, названного AES (Advanced Encryption Standard). К его разработке были подключены самые крупные центры криптологии всего мира.

К криптоалгоритмам - кандидатам на новый стандарт AES были предъявлены следующие требования:

- алгоритм должен быть симметричным;
- алгоритм должен быть блочным шифром;
- алгоритм должен иметь длину блока 128 бит и поддерживать три длины ключа: 128, 192 и 256 бит.

Дополнительно разработчикам криптоалгоритмов рекомендовалось:

- использовать операции, легко реализуемые как аппаратно (в микрочипах), так и программно (на персональных компьютерах и серверах);
- ориентироваться на 32-разрядные процессоры;
- не усложнять без необходимости структуру шифра для того, чтобы все заинтересованные стороны были в состоянии самостоятельно провести независимый криптоанализ алгоритма и убедиться, что в нем не заложено каких-либо недокументированных возможностей.

На этот конкурс было представлено 15 алгоритмов-претендентов, разработанных как известными в области криптографии организациями (RSA Security, Counterpane и т.д.), так и частными лицами. Итоги конкурса были подведены в октябре 2000 года. Победителем был объявлен алгоритм Rijndael, разработанный двумя криптографами из Бельгии - Винсентом Риджменом (Vincent Rijmen) и Джоан Даймен (Joan Daemen). Алгоритм Rijndael стал новым стандартом шифрования данных AES [7, 30].

Алгоритм AES не похож на большинство известных алгоритмов симметричного шифрования, структура которых носит название «сеть Фейстеля» и аналогична российскому ГОСТ 28147-89. В отличие от отечественного стандарта шифрования, алгоритм AES представляет каждый блок обрабатываемых данных в виде двухмерного байтового массива размером 4×4, 4×6 или 4×8 в зависимости от установленной длины блока (допускается использование нескольких фиксированных размеров шифруемого блока информации). Далее на соответствующих этапах производятся преобразования либо над независимыми столбцами, либо над независимыми строками, либо вообще над отдельными байтами.

Алгоритм AES состоит из определенного количества раундов (от 10 до 14 - это зависит от размера блока и длины ключа) и выполняет четыре преобразования:

- BS (ByteSub) - табличная замена каждого байта массива (рис.3.8);

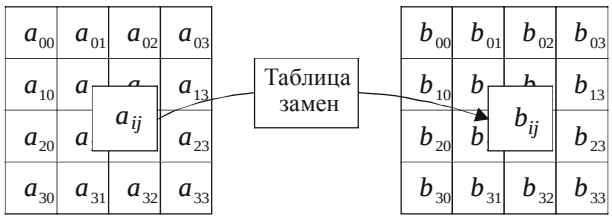

Рис.3.8. Преобразование BS (ByteSub) использует таблицу замен (подстановок) для обработки каждого байта массива State

• SR (ShiftRow) - сдвиг строк массива (рис.3.9).

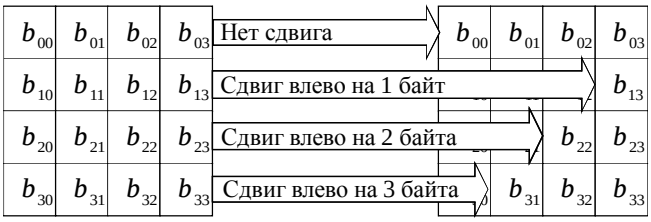

Рис.3.9. Преобразование SR (ShiftRow) циклически сдвигает три последних строки в массиве State

При этой операции первая строка остается без изменений, а остальные циклически побайтно сдвигаются влево на фиксированное число байт, зависящее от размера массива. Например, для массива размером 4×4 строки 2, 3 и 4 сдвигаются соответственно на 1, 2 и 3 байта;

• MC (MixColumn) - операция над независимыми столбцами массива (рис.3.10),

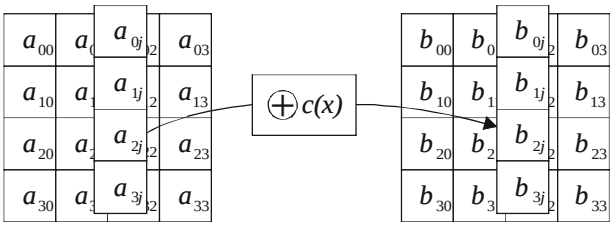

Рис.3.10. Преобразование MC (MixColumn) поочередно обрабатывает столбцы массива State

когда каждый столбец по определенному правилу умножается на фиксированную матрицу $c(x)$;

• AK (AddRoundKey) - добавление ключа. Каждый бит массива складывается по модулю 2 с соответствующим битом ключа раунда, который, в свою очередь, определенным образом вычисляется из ключа шифрования (рис.3.11).

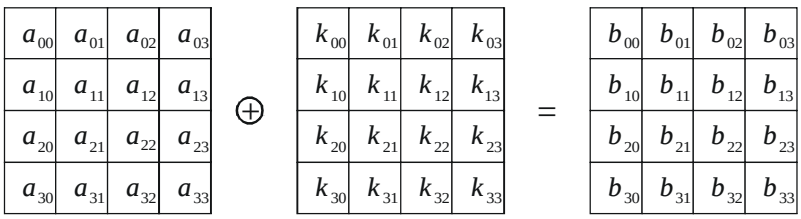

Рис.3.11. Преобразование AK (AddRoundKey) производит сложение XOR каждого столбца массива State со словом из ключевого набора

Эти преобразования воздействуют на массив State, который адресуется с помощью указателя ‘state’. Преобразование AddRoundKey использует дополнительный указатель для адресации ключа раунда Round Key.

Преобразование BS (ByteSub) является нелинейной байтовой подстановкой, которая воздействует независимо на каждый байт массива State, используя таблицу замен (подстановок) *S*-box.

В каждом раунде (с некоторыми исключениями) над шифруемыми данными поочередно выполняются перечисленные преобразования (рис.3.12). Исключения касаются первого и последнего раундов: перед первым раундом дополнительно выполняется операция AK, а в последнем раунде отсутствует MC. В

результате последовательность операций при зашифровании выглядит так: AK, {BS, SR, MC, AK} (повторяется R – 1 раз), BS, SR, AK.

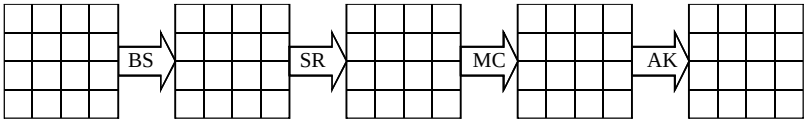

Рис.3.12. Раунд алгоритма AES

Количество раундов шифрования *R* в алгоритме AES переменное (10, 12 или 14 раундов) и зависит от размеров блока и ключа шифрования (для ключа также предусмотрено несколько фиксированных размеров).

Расшифрование выполняется с помощью следующих обратных операций.

1. Табличная замена BS обращается применением другой таблицы, являющейся инверсной относительно таблицы, применяемой при зашифровании.
2. Обратной операцией к SR является циклический сдвиг строк вправо, а не влево.
3. Обратная операция для MC - умножение по тем же правилам на другую матрицу $d(x)$, удовлетворяющую условию: $c(x) * d(x) = 1$.
4. Добавление ключа AK является обратным самому себе, поскольку в нем используется только операция XOR.

Эти обратные операции применяются при расшифровании в последовательности, обратной той, что использовалась при зашифровании.

Все преобразования в шифре AES имеют строгое математическое обоснование. Сама структура и последовательность операций позволяют выполнять данный алгоритм эффективно как на 8-битных так и на 32-битных процессорах. В структуре алгоритма заложена возможность параллельного исполнения некоторых операций, что может поднять скорость шифрования на многопроцессорных рабочих станциях в четыре раза.

Алгоритм Rijndael стал новым стандартом шифрования данных AES благодаря ряду преимуществ перед другими алгоритмами. Прежде всего он обеспечивает высокую скорость шифрования на всех платформах: как при программной, так и при аппаратной реализации. Кроме того, требования к ресурсам для его работы минимальны, что важно при его использовании в устройствах, обладающих ограниченными вычислительными возможностями.

Недостатком же алгоритма AES можно считать лишь свойственную ему нетрадиционную схему. Дело в том, что свойства алгоритмов, основанных на сети Фейстеля, хорошо исследованы, а AES, в отличие от них, может содержать скрытые уязвимости, которые могут обнаружиться только по прошествии какого-то времени с момента начала его широкого распространения.

Для шифрования данных применяются и другие блочные симметричные криптоалгоритмы.

Алгоритм IDEA (International Data Encryption Algorithm) - еще один 64-битный блочный шифр с длиной ключа 128 бит. Этот европейский стандарт криптоалгоритма предложен в 1990 году. Алгоритм IDEA по скорости не уступает алгоритму DES, а по стойкости к криптоанализу превосходит DES.

Алгоритм RC2 представляет собой 64-битовый блочный шифр с ключом переменной длины. Этот алгоритм приблизительно в 2 раза быстрее, чем DES. Может использоваться в тех же режимах, что и DES, включая тройное шифрование. Владельцем алгоритма является компания RSA Data Security.

Алгоритм RC5 представляет собой быстрый блочный шифр, который имеет размер блока 32, 64 или 128 бит, ключ длиной от 0 до 2048 бит. Алгоритм выполняет от 0 до 255 проходов. Алгоритмом владеет компания RSA Data Security.

Алгоритм Blowfish - это 64-битовый блочный шифр, имеет ключ переменного размера до 448 бит, выполняет 16 проходов, на каждом проходе осуществляются перестановки, зависящие от ключа, и подстановки, зависящие от ключа и данных. Этот алгоритм быстрее алгоритма DES.

3.2.4. Основные режимы работы блочного симметричного алгоритма

Большинство блочных симметричных криптоалгоритмов непосредственно преобразуют 64-битовый входной открытый текст в 64-битовый выходной шифрованный текст, однако данные редко ограничиваются 64 разрядами.

Чтобы воспользоваться блочным симметричным алгоритмом для решения разнообразных криптографических задач, разработаны четыре рабочих режима:

- электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

Эти рабочие режимы первоначально были разработаны для блочного алгоритма DES, но в любом из этих режимов могут работать и другие блочные криптоалгоритмы. Рассмотрим подробнее рабочие режимы ECB, CBC и CFB, получившие наибольшее распространение. В качестве примера будем использовать блочный алгоритм DES.

Режим «Электронная кодовая книга». Длинный файл разбивают на 64-битовые отрезки (блоки) по 8 байт. Каждый из этих блоков шифруют независимо с использованием одного и того же ключа шифрования (рис.3.13).

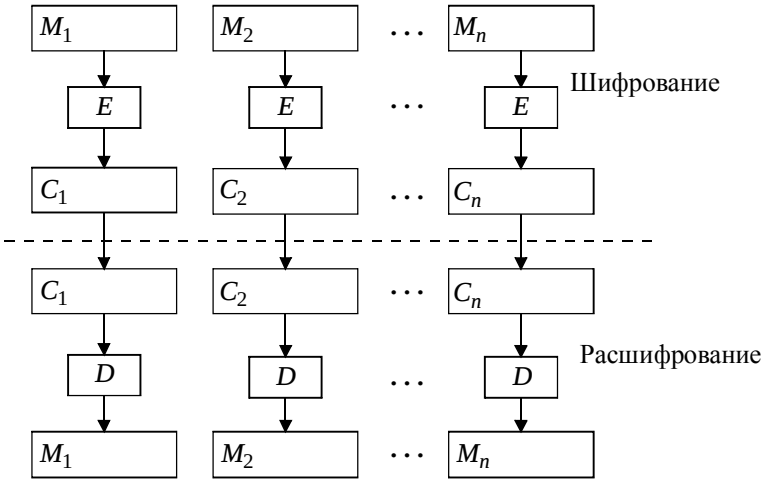

Рис.3.13. Схема работы блочного алгоритма в режиме электронной кодовой книги

Основное достоинство - простота реализации. Недостаток - относительно слабая устойчивость против криптоаналитических атак. Из-за фиксированного характера шифрования при ограниченной длине блока 64 бит возможно проведение криптоанализа «со словарем». Блок такого размера может повториться в сообщении вследствие большой избыточности в тексте на естественном языке. Это приводит к тому, что идентичные блоки открытого текста в сообщении будут представлены идентичными блоками шифртекста, что дает криптоаналитику некоторую информацию о содержании сообщения.

Режим «Сцепление блоков шифра». В этом режиме исходный файл M разбивается на 64-битовые блоки: $M = M_1M_2...M_n$. Первый блок M_1 складывается по модулю 2 с 64-битовым начальным вектором IV, который меняется ежедневно и держится в секрете (рис.3.14).

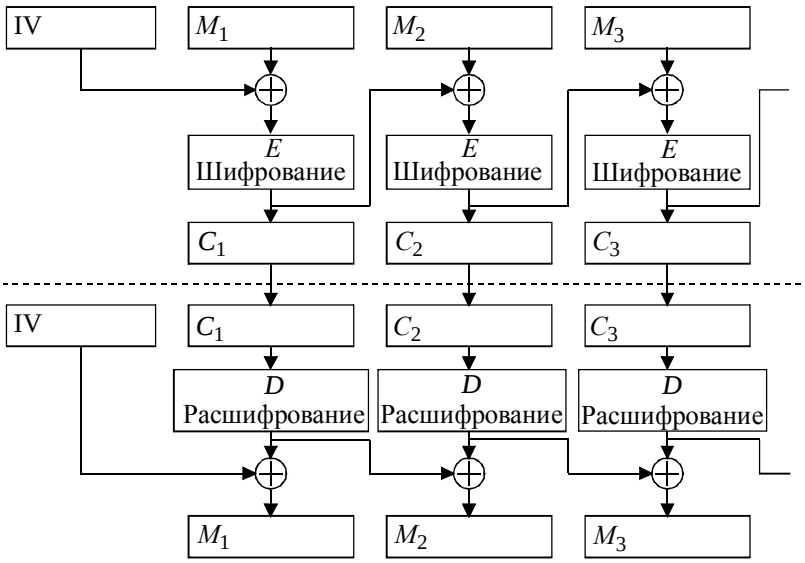

Рис.3.14. Схема работы блочного алгоритма в режиме сцепления блоков шифра

Полученная сумма затем шифруется с использованием ключа шифра, известного и отправителю, и получателю информации. Полученный 64-битовый блок шифртекста C_1 складывается по модулю 2 со вторым блоком текста, результат шифруется и получается второй 64-битовый блок шифртекста C_2 и т.д. Процедура повторяется до тех пор, пока не будут обработаны все блоки текста.

Таким образом, для всех $i = 1…n$ (n - число блоков) результат шифрования C_i определяется следующим образом: $C_i = E\ (M_i \oplus C_{i-1})$, где C_0 = IV - начальное значение шифра, равное начальному вектору (вектору инициализации).

Очевидно, что последний 64-битовый блок шифртекста является функцией секретного ключа, начального вектора и каждого бита открытого текста независимо от его длины. Этот блок шифртекста называют *кодом аутентификации сообщения* MAC (Message Authentication Code).

Код MAC может быть легко проверен получателем, владеющим секретным ключом и начальным вектором, путем повторения процедуры, выполненной отправителем. Посторонний, однако, не может осуществить генерацию MAC, который воспринялся бы получателем как подлинный, чтобы добавить его к ложному сообщению либо отделить MAC от истинного сообщения для использования его с измененным или ложным сообщением. Достоинство данного режима в том, что он не позволяет накапливаться ошибкам при передаче.

Блок M_i является функцией только C_{i-1} и C_i. Поэтому ошибка при передаче приведет к потере только двух блоков исходного текста.

Режим «Обратная связь по шифртексту». В этом режиме размер блока может отличаться от 64 бит (рис.3.15). Файл, подлежащий шифрованию (расшифровыванию), считывается последовательными блоками длиной k бит ($k = 1…64$).

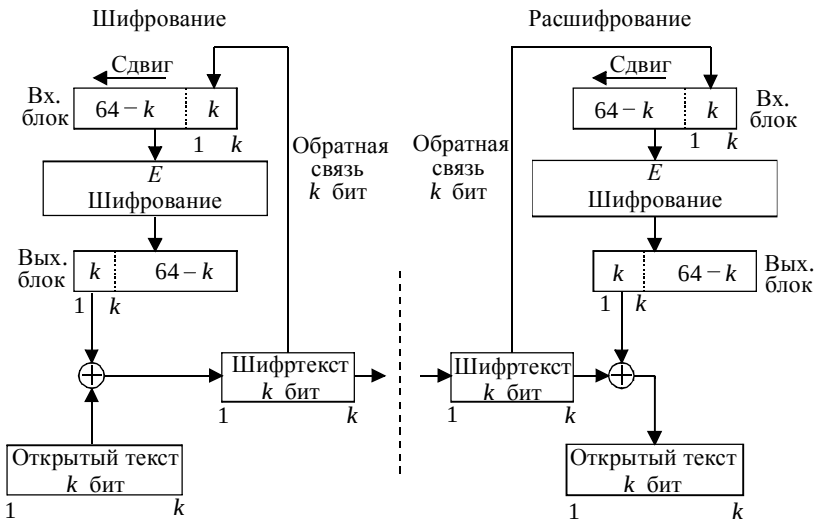

Рис.3.15. Схема работы блочного алгоритма в режиме обратной связи по шифртексту

Входной блок (64-битовый регистр сдвига) вначале содержит вектор инициализации, выровненный по правому краю.

Предположим, что в результате разбиения на блоки мы получили n блоков длиной k бит каждый (остаток дописывается нулями или пробелами). Тогда для любого $i = 1…n$ блок шифртекста $C_i = M_i \oplus P_{i-1}$, где P_{i-1} обозначает k старших бит предыдущего зашифрованного блока.

Обновление сдвигового регистра осуществляется путем удаления его старших k бит и записи C_i в регистр. Восстановление зашифрованных данных выполняют относительно просто: P_{i-1} и C_i вычисляются аналогичным образом и

$$M_i = C_i \oplus P_{i-1}.$$

Каждому из режимов (ECB, CBC, CFB, OFB) свойственны свои достоинства и недостатки, что обусловливает области их применения.

Режим ECB хорошо подходит для шифрования ключей. Режимы CBC и CFB позволяют использовать блочные симметричные алгоритмы для шифрования файлов, шифрования криптографических ключей в практике автоматизированного распространения ключей.

3.2.5. Особенности применения алгоритмов симметричного шифрования

Алгоритмы симметричного шифрования используют ключи относительно небольшой длины и могут быстро шифровать большие объемы данных. При симметричной методологии шифрования отправитель и получатель применяют один и тот же секретный ключ для осуществления процессов шифрования и расшифрования сообщения.

Алгоритмы симметричного шифрования строятся исходя из предположения, что зашифрованные данные не сможет прочитать никто из тех, кто не обладает ключом для их расшифрования. Если ключ не

был скомпрометирован, то при расшифровании автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, с помощью которого можно расшифровать информацию.

Алгоритмы симметричного шифрования применяются для абонентского шифрования данных, т.е. для шифрования информации, предназначенной для отправки кому-либо, например, через Интернет. Использование только одного секретного ключа для всех абонентов сети, конечно, недопустимо по соображениям безопасности: в случае компрометации (утери, хищения) ключа под угрозой будет находиться документооборот всех абонентов сети.

Для симметричных криптосистем актуальна проблема безопасного распределения симметричных секретных ключей. Всем системам симметричного шифрования присущи следующие недостатки:

- принципиальным является требование защищенности и надежности канала передачи секретного ключа для каждой пары участников информационного обмена;
- предъявляются повышенные требования к службе генерации и распределения ключей, обусловленные тем, что для n абонентов при схеме взаимодействия «каждый с каждым» требуется $n\cdot(n-1)/2$ ключей, т.е. зависимость числа ключей от числа абонентов является квадратичной. Например, для $n = 1000$ абонентов требуемое количество ключей будет равно $n\cdot(n-1)/2 = 499500$.

Поэтому без эффективной организации защищенного распределения ключей широкое использование обычной системы симметричного шифрования в больших сетях и, в частности, в глобальных сетях практически невозможно.

3.3. Асимметричные криптосистемы шифрования

Асимметричные криптографические системы были разработаны в 1970-х годах. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифрования применяются различные ключи:

- *открытый ключ* K используется для шифрования информации, вычисляется из секретного ключа k;
- *секретный ключ* k используется для расшифрования информации, зашифрованной с помощью парного ему открытого ключа K.

Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ k из открытого ключа K. Поэтому открытый ключ K может свободно передаваться по каналам связи.

Асимметричные системы называют еще двухключевыми криптографическими системами или криптосистемами с открытым ключом.

Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом показана на рис.3.16.

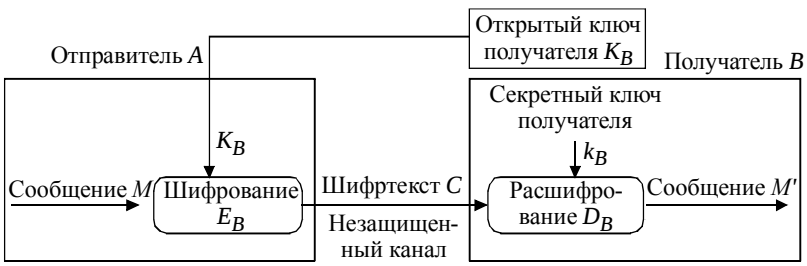

Рис.3.16. Обобщенная схема асимметричной криптосистемы шифрования

Для криптографического закрытия и последующего расшифрования передаваемой информации используются открытый и секретный ключи получателя B сообщения. В качестве ключа зашифрования должен использоваться открытый ключ получателя, а в качестве ключа расшифрования - его секретный ключ.

Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у его владельца; он должен быть надежно защищен от несанкционированного доступа (аналогично ключу шифрования в симметричных алгоритмах). Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа.

Процесс передачи зашифрованной информации в асимметричной криптосистеме осуществляется следующим образом.

1. *Подготовительный этап:*

- Абонент B генерирует пару ключей: секретный ключ k_B и открытый ключ K_B.
- Открытый ключ K_B посылается абоненту A и остальным абонентам (или делается доступным, например, на разделяемом ресурсе).

2. *Использование* - обмен информацией между абонентами A и B:

- Абонент A зашифровывает сообщение с помощью открытого ключа K_B абонента B и отправляет шифртекст абоненту B.
- Абонент B расшифровывает сообщение с помощью своего секретного ключа k_B. Никто другой (в том числе абонент A) не может расшифровать данное сообщение, так как не имеет секретного ключа абонента B. Защита информации в асимметричной криптосистеме основана на секретности ключа k_B получателя сообщения.

Отметим характерные особенности асимметричных криптосистем:

- открытый ключ K_B и криптограмма C могут быть отправлены по незащищенным каналам, т.е. противнику известны K_B и C;
- алгоритмы шифрования и расшифрования

$$E_B: M \to C,$$

$$D_B: C \to M$$

являются открытыми.

У. Диффи и М. Хеллман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы [8].

1. Вычисление пары ключей (K_B, k_B) получателем B должно быть простым.
2. Отправитель A, зная открытый ключ K_B и сообщение M, может легко вычислить криптограмму

$$C = E_{K_B}(M).$$

3. Получатель B, используя секретный ключ k_B и криптограмму C, может легко восстановить исходное сообщение

$$M = D_{k_B}(C).$$

4. Противник, зная открытый ключ K_B, при попытке вычислить секретный ключ k_B наталкивается на непреодолимую вычислительную проблему.
5. Противник, зная пару (K_B, C), при попытке вычислить исходное сообщение M наталкивается на непреодолимую вычислительную проблему.

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных функций.

Неформально *однонаправленную функцию* можно определить следующим образом [11]. Пусть X и Y - некоторые произвольные множества. Функция

$$f: X \to Y$$

является *однонаправленной*, если для всех $x \in X$ можно легко вычислить функцию

$$y = f(x), \text{ где } y \in Y.$$

И в то же время для большинства $y \in Y$ достаточно сложно получить значение $x \in X$, такое, что $f(x) = y$ (при этом полагают, что существует, по крайней мере, одно такое значение x).

Основным критерием отнесения функции f к классу однонаправленных функций является отсутствие эффективных алгоритмов обратного преобразования $Y \to X$.

В качестве примера однонаправленной функции можно указать *целочисленное умножение*. Прямая задача - вычисление произведения двух очень больших целых чисел P и Q, т.е. нахождение значения

$$N = P \cdot Q$$

является относительно несложной задачей для компьютера.

Обратная задача - факторизация, или разложение на множители большого целого числа, т.е. нахождение делителей P и Q большого целого числа $N = P \cdot Q$, является практически неразрешимой при достаточно больших значениях N. По современным оценкам теории чисел, при целом $N \approx 2^{664}$ и $P \approx Q$ для разложения числа N потребуется около 10^{23} операций, т.е. задача практически неразрешима на современных компьютеров.

Другой характерный пример однонаправленной функции - это *модульная экспонента с фиксированными основанием и модулем*. Пусть A и N - целые числа, такие, что $1 \le A < N$. Определим множество Z_N:

$$Z_N = \{0, 1, 2, \ldots N - 1\}.$$

Тогда модульная экспонента с основанием A по модулю N представляет собой функцию

$$f_{A,N}: Z_N \to Z_N,$$

$$f_{A,N}(x) = A^x \pmod N,$$

где X - целое число, $1 \le x \le N - 1$.

Существуют эффективные алгоритмы, позволяющие достаточно быстро вычислить значения функции $f_{A,N}(x)$.

Если $y = A^x$, то естественно записать $x = \log_A(y)$. Поэтому задачу обращения функции $f_{A,N}(x)$ называют задачей нахождения дискретного логарифма или задачей дискретного логарифмирования.

Задача дискретного логарифмирования формулируется следующим образом. Для известных целых A, N, y найти целое число x, такое, что

$$A^x \bmod N = y.$$

Алгоритм вычисления дискретного логарифма за приемлемое время пока не найден. Поэтому модульная экспонента считается однонаправленной функцией.

По современным оценкам теории чисел, при целых числах $A \approx 2^{664}$ и $N \approx 2^{664}$ решение задачи дискретного логарифмирования (нахождение показателя степени x для известного y) потребует около 10^{26} операций, т.е. эта задача имеет в 10^3 раз большую вычислительную сложность, чем задача разложения на множители. При увеличении длины чисел разница в оценках сложности задач возрастает.

Следует отметить, что пока не удалось доказать, что не существует эффективного алгоритма вычисления дискретного логарифма за приемлемое время. Исходя из этого, модульная экспонента отнесена к однонаправленным функциям условно, что, однако, не мешает с успехом применять ее на практике.

Вторым важным классом функций, используемых при построении криптосистем с открытым ключом, являются так называемые *однонаправленные функции с секретом*. Дадим неформальное определение такой функции. Функция

$$f: X \to Y$$

относится к классу однонаправленных функций с секретом в том случае, если она является однонаправленной и, кроме того, возможно эффективное вычисление обратной функции, если известен *секрет* (секретное число, строка или другая информация, ассоциирующаяся с данной функцией).

В качестве примера однонаправленной функции с секретом можно указать используемую в криптосистеме RSA модульную экспоненту с фиксированными модулем и показателем степени. Переменное основание модульной экспоненты используется для представления числового значения сообщения M либо криптограммы C.

Как и в случае симметричных криптографических систем, с помощью асимметричных криптосистем обеспечивается не только конфиденциальность, но также подлинность и целостность передаваемой информации. Подлинность и целостность любого сообщения обеспечивается формированием цифровой подписи этого сообщения и отправкой в зашифрованном виде сообщения вместе с цифровой подписью. Проверка соответствия подписи полученному сообщению после его предварительного расшифровывания представляет собой проверку целостности и подлинности принятого сообщения. Процедуры формирования и проверки электронной цифровой подписи рассмотрены в разделе 3.5.

Асимметричные криптографические системы обладают следующими важными преимуществами перед симметричными криптосистемами:

- в асимметричных криптосистемах решена сложная проблема распределения ключей между пользователями, так как каждый пользователь может сгенерировать свою пару ключей сам, а открытые ключи пользователей могут свободно публиковаться и распространяться по сетевым коммуникациям;
- исчезает квадратичная зависимость числа ключей от числа пользователей; в асимметричной криптосистеме количество используемых ключей связано с количеством абонентов линейной зависимостью (в системе из N пользователей используются $2N$ ключей), а не квадратичной, как в симметричных системах;
- асимметричные криптосистемы позволяют реализовать протоколы взаимодействия сторон, которые не доверяют друг другу, поскольку при использовании асимметричных криптосистем закрытый ключ должен быть известен только его владельцу.

Однако у асимметричных криптосистем существуют и недостатки:

- на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах функций;
- по сравнению с симметричным шифрованием, асимметричное существенно медленнее, поскольку при шифровании и расшифровке используются весьма ресурсоемкие операции. По этой же причине реализовать аппаратный шифратор с асимметричным алгоритмом существенно сложнее, чем реализовать аппаратно симметричный алгоритм;
- необходимо защищать открытые ключи от подмены. От подмены открытых ключей может защитить процедура сертификации открытых ключей.

3.3.1. Алгоритм шифрования RSA

Криптоалгоритм RSA предложили в 1978 году три автора: Р. Райвест (Rivest), А. Шамир (Shamir) и А. Адлеман (Adleman). Алгоритм получил свое название по первым буквам фамилий его авторов. Алгоритм

RSA стал первым алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи [11].

Надежность алгоритма RSA основывается на трудности факторизации больших чисел и трудности вычисления дискретных логарифмов в конечном поле.

В алгоритме RSA открытый ключ K_B, секретный ключ k_B, сообщение M и криптограмма C принадлежат множеству целых чисел

$$Z_N = \{0, 1, 2, ..., N - 1\},$$

где N - модуль:

$$N = P \cdot Q.$$

Здесь P и Q - случайные большие простые числа. Для обеспечения максимальной безопасности выбирают P и Q равной длины и хранят в секрете.

Множество Z_N с операциями сложения и умножения по модулю N образует арифметику по модулю N.

Открытый ключ K_B выбирают случайным образом так, чтобы выполнялись условия:

$$1< K_B \le \varphi(N), \text{ НОД } (K_B, \varphi(N)) = 1,$$

$$\varphi(N) = (P - 1)(Q - 1),$$

где $\varphi(N)$ - функция Эйлера.

Функция Эйлера $\varphi(N)$ указывает количество положительных целых чисел в интервале от 1 до N, которые взаимно просты с N.

Второе из указанных выше условий означает, что открытый ключ K_B и функция Эйлера $\varphi(N)$ должны быть взаимно простыми.

Далее, используя расширенный алгоритм Евклида, вычисляют секретный ключ k_B, такой, что

$$k_B \cdot K_B \equiv 1 \pmod{\varphi(N)}$$

или

$$k_B = K_B^{-1} \pmod{(P - 1)(Q - 1)}.$$

Это можно осуществить, так как получатель B знает пару простых чисел (P, Q) и может легко найти $\varphi(N)$. Заметим, что k_B и N должны быть взаимно простыми.

Открытый ключ K_B используют для шифрования данных, а секретный ключ k_B - для расшифрования.

Процедура шифрования определяет криптограмму C через пару (открытый ключ K_B, сообщение M) в соответствии со следующей формулой:

$$C = E_{K_B}(M) = M^{K^B} \pmod{N}.$$

В качестве алгоритма быстрого вычисления значения C используют ряд последовательных возведений в квадрат целого M и умножений на M с приведением по модулю N.

Расшифрование криптограммы C выполняют, используя пару (секретный ключ k_B, криптограмма C) по следующей формуле:

$$M = D_{k_B}(C) = C^{k^B} \pmod{N}.$$

Рассмотрим *процедуры шифрования и расшифрования в алгоритме RSA.* Предположим, что пользователь A хочет передать пользователю B сообщение в зашифрованном виде, используя алгоритм RSA. В таком случае пользователь A выступает в роли отправителя сообщения, а пользователь B - в роли получателя. Как отмечалось выше, криптосистему RSA должен сформировать получатель сообщения, т.е. пользователь B. Рассмотрим последовательность действий пользователя B и пользователя A.

1. Пользователь B выбирает два произвольных больших простых числа P и Q.
2. Пользователь B вычисляет значение модуля $N = P \cdot Q$.
3. Пользователь B вычисляет функцию Эйлера

$$\varphi(N) = (P - 1)(Q - 1)$$

и выбирает случайным образом значение открытого ключа K_B с учетом выполнения условий:

$$1< K_B \le \varphi(N), \text{ НОД } (K_B, \varphi(N)) = 1.$$

4. Пользователь B вычисляет значение секретного ключа k_B, используя расширенный алгоритм Евклида при решении сравнения

$$k_B \equiv K_B^{-1} \pmod{\varphi(N)}.$$

5. Пользователь B пересылает пользователю A пару чисел (N, K_B) по незащищенному каналу.

Если пользователь *A* хочет передать пользователю *B* сообщение *M*, он выполняет следующие шаги.

6. Пользователь *A* разбивает исходный открытый текст *M* на блоки, каждый из которых может быть представлен в виде числа

$$M_i = 0, 1, 2, ..., N - 1.$$

7. Пользователь *A* шифрует текст, представленный в виде последовательности чисел M_i по формуле

$$C_i = M_i^{K_B} \pmod N$$

и отправляет криптограмму

$$C_1, C_2, C_3, ..., C_i, ...$$

пользователю *B*.

8. Пользователь *B* расшифровывает принятую криптограмму

$$C_1, C_2, C_3, ..., C_i, ...,$$

используя секретный ключ k_B, по формуле

$$M_i = C_i^{k_B} \pmod N.$$

В результате будет получена последовательность чисел M_i, которые представляют собой исходное сообщение *M*. При практической реализации алгоритма RSA необходимо иметь возможность без существенных затрат генерировать большие простые числа, уметь оперативно вычислять значения ключей K_B и k_B.

Криптоалгоритм RSA всесторонне исследован и признан стойким при достаточной длине ключей. Следует отметить, что алгоритм RSA можно применять как для шифрования сообщений, так и для электронной цифровой подписи. Нетрудно видеть, что в асимметричной криптосистеме RSA количество используемых ключей связано с количеством абонентов линейной зависимостью (в системе из *N* пользователей используются 2*N* ключей), а не квадратичной, как в симметричных системах.

Сравнивая наиболее популярных представителей асимметричного и симметричного шифрования, следует отметить, что быстродействие RSA существенно ниже быстродействия 3DES, а программная и аппаратная реализация криптоалгоритма RSA гораздо сложнее, чем 3DES. Поэтому криптосистема RSA, как правило, используется при передаче небольшого объема сообщений.

3.3.2. Асимметричные криптосистемы на базе эллиптических кривых

К криптосистемам третьего тысячелетия, несомненно, следует отнести асимметричные криптосистемы на базе эллиптических кривых. Такие криптосистемы позволяют реализовать криптоалгоритм асимметричного шифрования, протокол выработки разделяемого секретного ключа для симметричного шифрования и криптоалгоритмы электронной цифровой подписи [1, 5]. Криптосистемы на базе эллиптических кривых имеют более высокую производительность и позволяют использовать существенно меньшие размеры ключей при сохранении требуемого уровня безопасности.

Для различных реализаций используются эллиптические кривые двух видов:

- эллиптическая кривая в конечном поле F_p , где *p* - простое число, $p > 3$;
- эллиптическая кривая в конечном поле F_2^m.

Эллиптическая кривая в конечном поле F_p. Пусть задано простое число $p > 3$. Тогда *эллиптической кривой E*, определенной над конечным простым полем F_p, называется множество пар чисел (x, y), $x \in F_p$, $y \in F_p$, удовлетворяющих тождеству

$$y^2 \equiv x^3 + ax + b \pmod p, \qquad (3.1)$$

где $a, b \in F_p$ и $4a^3 + 27b^2$ не сравнимо с нулем по модулю *p*.

Инвариантом эллиптической кривой называется величина *J(E)*, удовлетворяющая тождеству

$$J(E) = 1728 \frac{4a^3}{4a^3 + 27b^2} \pmod P.$$

Коэффициенты *a*, *b* эллиптической кривой *E*, по известному инварианту *J(E)*, определяются следующим образом:

$$\begin{cases} a \equiv 3k \pmod p, \\ b \equiv 2k \pmod p, \end{cases} \text{ где } k = \frac{J(E)}{1728 - J(E)} \pmod p, \quad J(E) \neq 0 \text{ или } 1728.$$

Пары *(x, y)*, удовлетворяющие тождеству (3.1), называются *точками эллиптической кривой E* ; *x* и *y* - соответственно *x*- и *y*-координатами точки.

Точки эллиптической кривой будем обозначать *Q*(*x*, *y*) или просто *Q*. Две точки эллиптической кривой равны, если равны их соответствующие *x*- и *y*-координаты.

На множестве всех точек эллиптической кривой *E* введем *операцию сложения*, которую будем обозначать знаком «+». Для двух произвольных точек $Q_1(x_1, y_1)$ и $Q_2(x_2, y_2)$ эллиптической кривой *E* рассмотрим несколько вариантов.

Пусть координаты точек Q_1 и Q_2 удовлетворяют условию $x_1 \neq x_2$. В этом случае их суммой будем называть точку $Q_3(x_3, y_3)$, координаты которой определяются сравнениями

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 \pmod p, \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod p, \end{cases}$$

где $\lambda \equiv \dfrac{y_2 - y_1}{x_2 - x_1} \pmod p$.

Если выполнены равенства $x_1 = x_2$ и $y_1 = y_2 \neq 0$, то определим координаты точки Q_3 следующим образом:

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 \pmod p, \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod p, \end{cases}$$

где $\lambda \equiv \dfrac{3x_1^2 + a}{2y_1} \pmod p$.

В случае, когда выполнено условие $x_1 = x_2$ и $y_1 = -y_2 \pmod p$, сумму точек Q_1 и Q_2 будем называть *нулевой точкой O*, не определяя ее *x*- и *y*-координаты. В этом случае точка Q_2 называется *отрицанием* точки Q_1. Для нулевой точки *O* выполнены равенства

$$Q + O = O + Q = Q,$$

где *Q* - произвольная точка эллиптической кривой *E*.

Относительно введенной операции сложения множество всех точек эллиптической кривой *E*, вместе с нулевой точкой, образуют *конечную абелеву (коммутативную) группу порядка m*, для которого выполнено неравенство

$$p + 1 - 2\sqrt{p} \le m \le p + 1 + 2\sqrt{p}.$$

Точка *Q* называется точкой кратности *k* или просто кратной точкой эллиптической кривой *E*, если для некоторой точки *P* выполнено равенство

$$Q = \underbrace{P + P + \ldots + P}_{k} = kP.$$

Эллиптическая кривая в конечном поле F_2^m. Такая кривая определяется соотношением

$$y^2 + xy \equiv x^3 + ax^2 + b$$

при ненулевом *b*.

Эллиптической кривой $E(F_{2^m})$ является группа решений (x, y), $x \in F_{2^m}, y \in F_{2^m}$, приведенного выше соотношения при определенных значениях *a* и *b*, а также нулевая точка *O*.

Аналогично группе эллиптической кривой $E(F_p)$ множество всех точек эллиптической кривой $E(F_{2^m})$ вместе с нулевой точкой образуют конечную абелеву группу.

С помощью описанных выше правил сложения можно вычислить точку *kP* для любого целого числа *k* и любой точки *P* эллиптической кривой.

Однако решение обратной задачи - нахождение числа *k* по известным точкам *P* и *kP* является трудноразрешимой проблемой. Данную задачу называют *проблемой дискретного логарифма эллиптической кривой ECDLP (Elliptic Curve Discrete Logariphm Problem).* Решение проблемы ECDLP является значительно более сложным, чем решение проблемы дискретного логарифмирования (нахождение числа *x* по заданному числу $y = g^x \bmod p$ при известных основании *g* и модуле *p*), на которой базируются RSA-подобные асимметричные криптосистемы.

Сложность решения проблемы ECDLP обусловлена ресурсоемкостью операций сложения и дублирования точек, с помощью которых вычисляется kP, как видно из приведенных выше формул. Отсюда следует возможность применения более коротких ключей. Например, ключу размером 1024 бит алгоритма DSA соответствует по криптостойкости ключ размером 160 бит алгоритма ECDSA (DSA на эллиптических кривых).

Существует несколько реализаций известных криптоалгоритмов на базе эллиптических кривых (стандартизованы в IEEE P1363).

3.3.3. Алгоритм асимметричного шифрования ECES

В алгоритме ECES *(Elliptic Curve Encryption Scheme)* сначала должны быть определены следующие параметры, являющиеся открытой информацией, общей для всех пользователей системы [1, 5]:

- конечное поле F_q;
- эллиптическая кривая $E(F_q)$;
- большой простой делитель количества точек кривой n;
- точка P, координаты которой должны иметь тот же порядок, что и число n.

Каждый пользователь системы генерирует пару ключей следующим образом:

- выбирается случайное целое число d, $1 < d < n - 1$;
- вычисляется точка $Q = dP$.

Секретным ключом пользователя является число d, открытым ключом - точка Q.

Зашифрование сообщения (пользователь A шифрует сообщение M для пользователя B):

- сообщение разбивается на блоки M_i, которые определенным образом дополняются слева (длина каждого блока равна $2L - 16$ бит, где L равно ближайшему большему целому от $\log_2 q$);
- полученный блок разбивается на 2 части равной длины: m_{i1} и m_{i2};
- выбирается случайное целое число k, $1 < k < n - 1$;
- вычисляется точка $(x_1, y_1) = kP$;
- вычисляется точка $(x_2, y_2) = kQ_B$;
- с помощью определенного преобразования из m_{i1}, m_{i2} и x_2 получают c_1 и c_2;
- зашифрованные данные: (x_1, y_1, c_1, c_2).

Расшифрование сообщения (пользователь B расшифровывает полученное от пользователя A зашифрованное сообщение):

- вычисляется точка $(x_2, y_2) = d(x_1, y_1)$;
- восстанавливается исходное сообщение m_{i1}, m_{i2} из c_1, c_2 и x_2.

3.4. Функции хэширования

Функция хэширования (хэш-функция) представляет собой преобразование, на вход которого подается сообщение переменной длины M, а выходом является строка фиксированной длины $h(M)$. Иначе говоря, хэш-функция $h(\cdot)$ принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение (хэш) $H = h(M)$ фиксированной длины (рис.3.17).

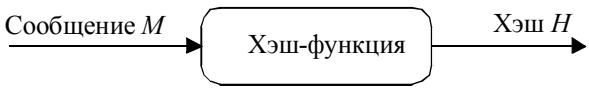

Рис.3.17. Схема формирования хэша $H = h(M)$

Хэш-значение $h(M)$ - это *дайджест сообщения* M, т.е. сжатое двоичное представление основного сообщения M произвольной длины. Хэш-значение $h(M)$ формируется функцией хэширования.

Функция хэширования позволяет сжать подписываемый документ M до 128 и более бит (в частности, 128 или 256 бит), тогда как M может быть размером в мегабайт или более. Следует отметить, что значение хэш-функции $h(M)$ зависит сложным образом от документа M и не позволяет восстановить сам документ M.

Функция хэширования должна обладать следующими свойствами.

1. Хэш-функция может быть применена к аргументу любого размера.
2. Выходное значение хэш-функции имеет фиксированный размер.
3. Хэш-функцию $h(x)$ достаточно просто вычислить для любого x. Скорость вычисления хэш-функции должна быть такой, чтобы скорость выработки и проверки ЭЦП при использовании хэш-функции была значительно больше, чем при использовании самого сообщения.
4. Хэш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким, как вставки, выбросы, перестановки и т.п.

5. Хэш-функция должна быть однонаправленной, т.е. обладать свойством необратимости, иными словами, задача подбора документа M', который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима.

6. Вероятность того, что значения хэш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала, т.е. для любого фиксированного x с вычислительной точки зрения невозможно найти $x' \neq x$, такое, что $h(x') = h(x)$.

Теоретически возможно, что два различных сообщения могут быть сжаты в одну и ту же свертку (так называемая коллизия или «столкновение»). Поэтому для обеспечения стойкости функции хэширования необходимо предусмотреть способ избегать столкновений. Полностью столкновений избежать нельзя, поскольку в общем случае количество возможных сообщений превышает количество возможных выходных значений функции хэширования. Однако вероятность столкновения должна быть низкой.

Свойство 5 эквивалентно тому, что $h(\cdot)$ является односторонней функцией. Свойство 6 гарантирует, что не может быть найдено другое сообщение, дающее ту же свертку. Это предотвращает фальсификацию сообщения.

Таким образом, функция хэширования может использоваться для обнаружения изменений сообщения, т.е. она может служить для формирования *криптографической контрольной суммы* (также называемой кодом обнаружения изменений или *кодом аутентификации сообщения*). В этом качестве хэш-функция используется для контроля целостности сообщения, при формировании и проверке электронной цифровой подписи.

Хэш-функции широко используются также в целях аутентификации пользователей. В ряде технологий информационной безопасности применяется своеобразный прием шифрования - *шифрование с помощью односторонней хэш-функции*. Своеобразие этого шифрования заключается в том, что оно, по существу, является односторонним, т.е. не сопровождается обратной процедурой - расшифрованием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования на основе хэш-функции [11].

Известные функции хэширования:

- отечественный стандарт ГОСТ Р34.11-94 [1]. Вычисляет хэш размером 32 байт;
- MD (Message Digest) - ряд алгоритмов хэширования, наиболее распространенных в мире. Каждый из них вырабатывает 128-битовый хэш-код. Алгоритм MD2 - самый медленный из них, MD4 - самый быстрый. Алгоритм MD5 является модификацией MD4, при которой пожертвовали скоростью ради увеличения безопасности. Алгоритм MD5 применяется в последних версиях Microsoft Windows для преобразования пароля пользователя в 16-байтное число [1];
- SHA (Secure Hash Algorithm) - это алгоритм вычисления дайджеста сообщений, вырабатывающий 160-битовый *хэш-код* входных данных, широко распространен в мире, используется во многих сетевых протоколах защиты информации.

Хэш-функции широко используются также для аутентификации пользователей. Существует множество криптографических протоколов, основанных на применении хэш-функций (см. разделы 3.5 и 3.6).

Отечественным стандартом генерирования хэш-функции является ***алгоритм ГОСТ Р 34.11-94***. Этот стандарт является обязательным для применения в качестве алгоритма хэширования в государственных организациях РФ и ряде коммерческих организаций. Коротко данный алгоритм хэширования можно описать следующим образом (рис.3.18).

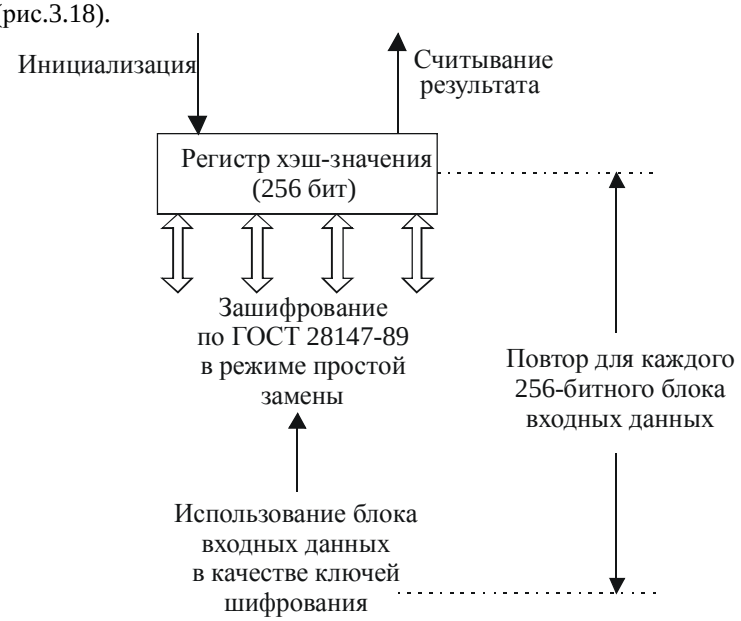

Рис.3.18. Хэширование по алгоритму ГОСТ Р 34.11-94

Шаг 1. Инициализация регистра хэш-значения. Если длина сообщения не превышает 256 бит - переход к шагу 3, если превышает - переход к шагу 2.

Шаг 2. Итеративное вычисление хэш-значения блоков хэшируемых данных по 256 бит с использованием хранящегося в регистре хэш-значения предыдущего блока. Вычисление включает в себя следующие действия:

- генерацию ключей шифрования на основе блока хэшируемых данных;
- зашифрование хранящегося в регистре хэш-значения в виде четырех блоков по 64 бит по алгоритму ГОСТ 28147-89 в режиме простой замены;
- перемешивание результата.

Вычисление производится до тех пор, пока длина необработанных входных данных не станет меньше или равной 256 бит. В этом случае - переход к шагу 3.

Шаг 3. Дополнение битовыми нулями необработанной части сообщения до 256 бит. Вычисление хэш-значения аналогично шагу 2. В результате в регистре оказывается искомое хэш-значение.

3.5. Электронная цифровая подпись

Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. При таком обмене электронными документами существенно снижаются затраты на обработку и хранение документов, убыстряется их поиск. Но возникает проблема аутентификации автора электронного документа и самого документа, т.е. установления подлинности автора и отсутствия изменений в полученном электронном документе.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

- *активный перехват* - нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
- *«маскарад»* - абонент *C* посылает документ абоненту *B* от имени абонента *A*;
- *ренегатство* - абонент *A* заявляет, что не посылал сообщения абоненту *B*, хотя на самом деле послал;
- *подмена* - абонент *B* изменяет или формирует новый документ и заявляет, что получил его от абонента *A*;
- *повтор* - абонент *C* повторяет ранее переданный документ, который абонент *A* посылал абоненту *B*.

Эти виды злоумышленных действий могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, частным лицам, применяющим в своей деятельности компьютерные информационные технологии.

Проблему проверки целостности сообщения и подлинности автора сообщения позволяет эффективно решить методология электронной цифровой подписи.

3.5.1. Основные процедуры цифровой подписи

Функционально цифровая подпись аналогична обычной рукописной подписи и обладает ее основными достоинствами:

- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
- гарантирует целостность подписанного текста.

ЭЦП представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом. ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности цифровой подписи. ЭЦП реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа.

Система ЭЦП включает две основные процедуры:

- процедуру формирования цифровой подписи;
- процедуру проверки цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи - открытый ключ отправителя.

Процедура формирования цифровой подписи. На подготовительном этапе этой процедуры абонент A - отправитель сообщения генерирует пару ключей: секретный ключ k_A и открытый ключ K_A. Открытый ключ K_A вычисляется из парного ему секретного ключа k_A. Открытый ключ K_A рассылается остальным абонентам сети (или делается доступным, например, на разделяемом ресурсе) для использования при проверке подписи.

Для формирования цифровой подписи отправитель A прежде всего вычисляет значение хэш-функции $h(M)$ подписываемого текста M (рис.3.19).

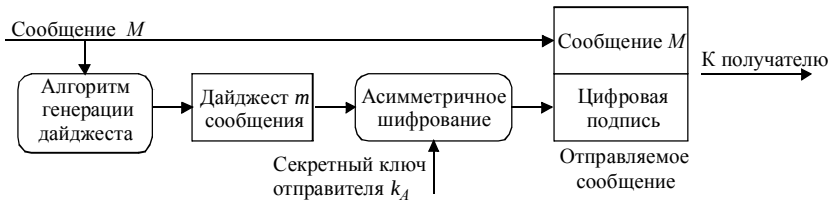

Рис.3.19. Схема формирования электронной цифровой подписи

Хэш-функция служит для сжатия исходного подписываемого текста M в дайджест m - относительно короткое число, состоящее из фиксированного небольшого числа битов и характеризующее весь текст M в целом.

Далее отправитель A шифрует дайджест m своим секретным ключом k_A. Получаемая при этом пара чисел представляет собой цифровую подпись для данного текста M. Сообщение M вместе с цифровой подписью отправляется в адрес получателя.

Процедура проверки цифровой подписи. Абоненты сети могут проверить цифровую подпись полученного сообщения M с помощью открытого ключа отправителя K_A этого сообщения (рис.3.20).

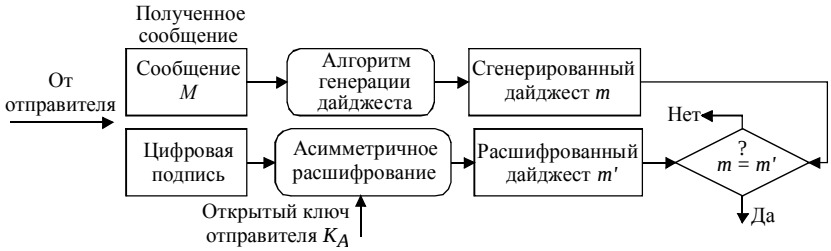

Рис.3.20. Схема проверки электронной цифровой подписи

При проверке ЭЦП абонент B - получатель сообщения M расшифровывает принятый дайджест m открытым ключом K_A отправителя A. Кроме того, получатель сам вычисляет с помощью хэш-функции $h(M)$ дайджест m' принятого сообщения M и сравнивает его с расшифрованным. Если эти два дайджеста m и m' совпадают, то цифровая подпись является подлинной. В противном случае либо подпись подделана, либо изменено содержание сообщения.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания. Поэтому необходимо защитить секретный ключ подписывания от несанкционированного доступа. Секретный ключ ЭЦП аналогично ключу симметричного шифрования рекомендуется хранить на персональном ключевом носителе в защищенном виде.

Электронная цифровая подпись представляет собой уникальное число, зависящее от подписываемого документа и секретного ключа абонента. В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей.

Помещаемая в подписываемый файл (или в отдельный файл электронной подписи) структура ЭЦП обычно содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация добавляется к документу до вычисления ЭЦП, что обеспечивает и ее целостность. Каждая подпись содержит следующую информацию:

- дату подписи;
- срок окончания действия ключа данной подписи;
- информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
- идентификатор подписавшего (имя открытого ключа);
- собственно цифровую подпись.

Важно отметить, что с точки зрения конечного пользователя процесс формирования и проверки цифровой подписи отличается от процесса криптографического закрытия передаваемых данных следующими особенностями.

При формировании цифровой подписи используются закрытый ключ отправителя, тогда как при зашифровании используется открытый ключ получателя. При проверке цифровой подписи используется открытый ключ отправителя, а при расшифровании - закрытый ключ получателя.

Проверить сформированную подпись может любое лицо, так как ключ проверки подписи является открытым. При положительном результате проверки подписи делается заключение о подлинности и целостности полученного сообщения, т.е. о том, что это сообщение действительно отправлено тем или иным отправителем и не было модифицировано при передаче по сети. Однако если пользователя интересует, не является ли полученное сообщение повторением ранее отправленного или не было ли оно задержано на пути следования, он должен проверить дату и время его отправки, а при наличии - порядковый номер.

Аналогично асимметричному шифрованию необходимо обеспечить невозможность подмены открытого ключа, используемого для проверки ЭЦП. Если предположить, что злоумышленник n имеет доступ к открытым ключам, которые хранит на своем компьютере абонент B, в том числе к открытому ключу K_A абонента A, то он может выполнить следующие действия:

- прочитать из файла, в котором содержится открытый ключ K_A, идентификационную информацию об абоненте A;
- сгенерировать собственную пару ключей k_n и K_n, записав в них идентификационную информацию абонента A;
- подменить хранящийся у абонента B открытый ключ K_A своим открытым ключом K_n, но содержащим идентификационную информацию абонента A.

После этого злоумышленник n может посылать документы абоненту B, подписанные своим секретным ключом k_n. При проверке подписи этих документов абонент B будет считать, что документы подписаны абонентом A и их ЭЦП верна, т.е. они не были модифицированы кем-либо. До выяснения отношений непосредственно с абонентом A у абонента B может не появиться сомнений в полученных документах. Открытые ключи ЭЦП можно защитить от подмены с помощью соответствующих цифровых сертификатов.

Сегодня существует большое количество алгоритмов ЭЦП.

3.5.2. Алгоритм цифровой подписи ГОСТ Р 34.10-94

Данный алгоритм цифровой подписи является первым отечественным стандартом цифровой подписи и обозначается как ГОСТ Р 34.10-94 [11]. Алгоритм цифровой подписи, определяемый этим стандартом, концептуально близок к американскому алгоритму цифровой подписи DSA (Digital Signature Algorithm) [1]. В алгоритме цифровой подписи ГОСТ Р 34.10-94 используются следующие параметры:

p - большое простое число длиной от 509 до 512 бит либо от 1020 до 1024 бит;

q - простой сомножитель числа $(p-1)$, имеющий длину 254…256 бит.

a - любое число, меньшее $(p-1)$, причем такое, что $a^q \bmod p = 1$;

x - некоторое число, меньшее q;

$y = a^x \bmod p$.

Кроме того, этот алгоритм использует однонаправленную хэш-функцию $H(x)$. Стандарт ГОСТ Р 34.11-94 определяет хэш-функцию, основанную на использовании стандартного симметричного алгоритма ГОСТ 28147-89.

Первые три параметра p, q и a являются открытыми и могут быть общими для всех пользователей сети. Число x является секретным ключом. Число y является открытым ключом.

Чтобы подписать некоторое сообщение m, а затем проверить подпись, выполняются следующие шаги.

Шаг 1. Пользователь A генерирует случайное число k, причем $k < q$.

Шаг 2. Пользователь A вычисляет значения

$$r = (a^k \bmod p) \bmod q,$$

$$s = (x \cdot r + k(H(m))) \bmod q.$$

Если $H(m) \bmod q = 0$, то значение $H(m) \bmod q$ принимают равным единице. Если $r = 0$, то выбирают другое значение k и начинают снова.

Цифровая подпись представляет собой два числа:

$$r \bmod 2^{256} \text{ и } s \bmod 2^{256}.$$

Пользователь A отправляет эти числа пользователю B.

Шаг 3. Пользователь B проверяет полученную подпись, вычисляя

$$v = H(m)^{q-2} \bmod q,$$

$$z_1 = (s \cdot v) \bmod q,$$

$$z_2 = ((q - r) \cdot v) \bmod q,$$

$$u = ((a^{z_1} \cdot y^{z_2}) \bmod p) \bmod q.$$

Если $u = r$, то подпись считается верной.

Различие между этим алгоритмом и алгоритмом DSA заключается в том, что в DSA

$$s = (k^{-1} (x \cdot r + (H(m)))) \bmod q,$$

это приводит к другому уравнению верификации.

Следует также отметить, что в отечественном стандарте ЭЦП параметр q имеет длину 256 бит. Западных криптографов вполне устраивает q длиной примерно 160 бит. Различие в значениях параметра q является отражением стремления разработчиков отечественного стандарта к получению более безопасной подписи. Этот стандарт вступил в действие с начала 1995 года.

3.5.3. Алгоритм цифровой подписи ECDSA

В алгоритме ЭЦП ECDSA (Elliptic Curve Digital Signature Algorithm) определение параметров системы и генерация ключей аналогичны алгоритму асимметричного шифрования ECES.

Генерация ЭЦП (пользователь A подписывает сообщение M):

- вычисляются хэш-сообщения $H(M)$;
- выбирается случайное целое число k, взаимно простое с n (т.е. не имеющее других, общих с n делителей, кроме 1; поскольку n является простым числом по определению, данное условие выполняется автоматически), $1 < k < n - 1$;
- вычисляется точка $(x_1, y_1) = kP$ и $r = x_1 \bmod n$. В случае, если $r = 0$, повторяется выбор k;
- вычисляется $s = k^{-1} (H(M) + rd) \bmod n$;
- цифровой подписью сообщения M является пара чисел (r, s).

Проверка ЭЦП (пользователь B проверяет ЭЦП пользователя A под сообщением M):

- если $r = 0$, то полученная ЭЦП неверна;
- вычисляются хэш-сообщения $H(M)$;
- вычисляются $u = s^{-1} H(M) \bmod n$ и $v = s^{-1} r \bmod n$;
- вычисляется точка $(x_1, y_1) = uP + vQ$;
- вычисляется $r' = x_1 \bmod n$;
- ЭЦП считается верной, если $r' = r$.

3.5.4. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001

Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001 был принят в 2001 г. [1]. Этот стандарт разработан взамен первого стандарта цифровой подписи ГОСТ Р 34.10-94. Необходимость разработки стандарта ГОСТ Р 34.10-2001 вызвана потребностью в повышении стойкости электронной цифровой подписи к несанкционированным изменениям. Стойкость ЭЦП основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11.

Принципиальное отличие нового стандарта от предыдущего ГОСТ Р 34.10-94 состоит в том, что все вычисления при генерации и проверке ЭЦП в новом алгоритме производятся в группе точек эллиптической кривой, определенной над конечным полем F_p.

Принадлежность точки (пары чисел x и y) к данной группе определяется следующим соотношением:

$$y^2 \equiv x^3 + ax + b (\bmod p),$$

где модуль системы p является простым числом больше 3, а a и b являются константами, удовлетворяющими следующим соотношениям: $a, b \in F_p$ и $4a^3 + 27b^2$ не сравнимо с нулем по модулю p.

При этом следует отметить, что принципы вычислений по данному алгоритму схожи с предшествующим отечественным стандартом ЭЦП: генерируется случайное число x, с его помощью вычисляется r-часть ЭЦП, затем вычисляется s-часть ЭЦП из r-части, x, значения секретного ключа и хэш-значения подписываемых данных. При проверке же подписи аналогичным вышеописанному образом проверяется соответствие определенным соотношениям r, s, открытого ключа и хэш-значения информации, подпись которой проверяется. Подпись считается неверной, если соотношения не соблюдаются. Математические подробности реализации этого алгоритма приводятся ниже.

Обозначения. В данном стандарте использованы следующие обозначения:

V_{256} - множество всех двоичных векторов длиной 256 бит;

V_∞ - множество всех двоичных векторов произвольной конечной длины;

Z - множество всех целых чисел;

p - простое число, $p > 3$;

F_p - конечное простое поле, представляемое как множество из p целых чисел $\{0, 1, \ldots, p - 1\}$;

$b \pmod p$ - минимальное неотрицательное число, сравнимое с b по модулю p;

M - сообщение пользователя, $M \in V_\infty$;

$(\bar{h}_1 \| \bar{h}_2)$ - конкатенация (объединение) двух двоичных векторов;

a, b - коэффициенты эллиптической кривой;

m - порядок группы точек эллиптической кривой;

q - порядок подгруппы группы точек эллиптической кривой;

O - нулевая точка эллиптической кривой;

P - точка эллиптической кривой порядка q;

d - целое число - ключ подписи;

Q - точка эллиптической кривой - ключ проверки;

w - цифровая подпись под сообщением M.

Общие положения. Механизм цифровой подписи реализуется посредством двух основных процессов:
формирование цифровой подписи;
проверка цифровой подписи.

В *процессе формирования цифровой подписи* в качестве исходных данных используются сообщение M, ключ подписи d и параметры схемы ЭЦП, а в результате формируется цифровая подпись w.

Ключ подписи d является элементом секретных данных, специфичным для субъекта и используемым только данным субъектом в процессе формирования цифровой подписи.

Параметры схемы ЭЦП - элементы данных, общие для всех субъектов схемы цифровой подписи, известные или доступные всем этим субъектам.

Электронная цифровая подпись w представляет собой строку бит, полученную в результате процесса формирования подписи. Данная строка имеет внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

В *процессе проверки цифровой подписи* в качестве исходных данных используются подписанное сообщение, ключ проверки Q и параметры схемы ЭЦП, а результатом проверки является заключение о правильности или ошибочности цифровой подписи.

Ключ проверки Q является элементом данных, математически связанным с ключом подписи d и используемым проверяющей стороной в процессе проверки цифровой подписи.

Схематическое представление подписанного сообщения показано на рис.3.21.

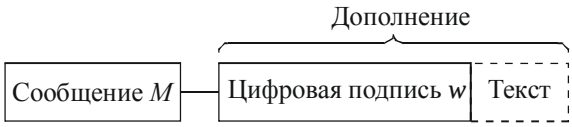

Рис.3.21. Схема подписанного сообщения

Поле «Текст», показанное на рис.3.21 и дополняющее поле «Цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в данном стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем, а также хэш-функции.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Алгоритм вычисления хэш-функции установлен в ГОСТ Р 34.11.

Цифровая подпись, представленная в виде двоичного вектора длиной 512 бит, должна вычисляться и проверяться с помощью определенных наборов правил, изложенных ниже.

Параметры схемы цифровой подписи, необходимые для ее формирования и проверки, следующие:

- простое число p - модуль эллиптической кривой, удовлетворяющее неравенству $p > 2^{255}$. Верхняя граница данного числа должна определяться при конкретной реализации схемы цифровой подписи;
- эллиптическая кривая E, задаваемая своим инвариантом $J(E)$ или коэффициентами $a, b \in F_p$;
- целое число m - порядок группы точек эллиптической кривой E;
- простое число q - порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} m = nq,\ n \in Z,\ n \geq 1, \\ 2^{254} < q < 2^{256}; \end{cases}$$

- точка $P \neq 0$ эллиптической кривой E с координатами (x_P, y_P), удовлетворяющая равенству $qP = 0$;
- хэш-функция $h(\cdot): V_\infty \to V_{256}$, отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные векторы длиной 256 бит. Хэш-функция определена в ГОСТ Р 34.11.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

- ключом подписи - целым числом d, удовлетворяющим неравенству $0 < d < q$;
- ключом проверки - точкой эллиптической кривой Q с координатами (x_q, y_q), удовлетворяющей равенству $dP = Q$.

На приведенные выше параметры схемы цифровой подписи налагаются следующие требования:

- должно быть выполнено условие $p^t \neq 1 \pmod p$, для всех целых t = 1, 2, ... B, где B удовлетворяет неравенству $B \geq 31$;
- должно быть выполнено неравенство $m \neq p$;
- инвариант кривой должен удовлетворять условию $J(E) \neq 0$ или 1728.

Двоичные векторы. Для определения процессов формирования и проверки цифровой подписи необходимо установить соответствие между целыми числами и двоичными векторами длиной 256 бит.

Рассмотрим следующий двоичный вектор длиной 256 бит, в котором младшие биты расположены справа, а старшие - слева:

$$\bar{h} = (\alpha_{255}, ..., \alpha_0), \bar{h} \in V_{256},$$

где $\alpha_i, i = 0,...,255$, равно либо 1, либо 0. Будем считать, что число $\alpha \in Z$ *соответствует* двоичному вектору $\bar{h}$, если выполнено равенство

$$\alpha = \sum_{i=0}^{255} \alpha_i 2^i .$$

Для двух двоичных векторов $\bar{h}_1$ и $\bar{h}_2$, соответствующих целым числам α и β, определим операцию конкатенации (объединения) следующим образом. Пусть

$$\bar{h}_1 = (\alpha_{255}, ..., \alpha_0),$$
$$\bar{h}_2 = (\beta_{255}, ..., \beta_0),$$

тогда их объединение имеет вид

$$\bar{h}_1 \| \bar{h}_2 = (\alpha_{255}, ..., \alpha_0, \beta_{255}, ..., \beta_0)$$

и представляет собой двоичный вектор длиной 512 бит, составленный из коэффициентов векторов $\bar{h}_1$ и $\bar{h}_2$.

С другой стороны, приведенные формулы определяют способ разбиения двоичного вектора $\bar{h}$ длиной 512 бит на два двоичных вектора длиной 256 бит, конкатенацией которых он является.

Основные процессы. В данном разделе определены процессы формирования и проверки электронной цифровой подписи под сообщением пользователя. Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры схемы цифровой подписи, удовлетворяющие приведенным выше требованиям.

Кроме того, каждый пользователь должен иметь ключ подписи d и ключ проверки подписи $Q(x_q, y_q)$, которые также должны удовлетворять приведенным выше требованиям.

Формирование цифровой подписи. Для получения цифровой подписи под сообщением $M \in V_\infty$ необходимо выполнить следующие действия (шаги).

Шаг 1. Вычислить хэш-код сообщения M:

$$\bar{h} = h(M).$$

Шаг 2. Вычислить целое число α, двоичным представлением которого является вектор $\bar{h}$, и определить значение

$$e \equiv \alpha \pmod q .$$

Если $e = 0$, то определить $e = 1$.

Шаг 3. Сгенерировать случайное (псевдослучайное) целое число k, удовлетворяющее неравенству

$$0 < k < q .$$

Шаг 4. Вычислить точку эллиптической кривой $C = kP$ и определить

$$r \equiv x_c \pmod q,$$

где x_c - x-координата точки C. Если $r = 0$, то вернуться к шагу 3.

Шаг 5. Вычислить значение

$$s \equiv (rd + ke) (\mathrm{mod}\, q) .$$

Если $s = 0$, то вернуться к шагу 3.

Шаг 6. Вычислить двоичные векторы $\bar{r}$ и $\bar{s}$, соответствующие r и s, и определить цифровую подпись $w = (\bar{r} \| \bar{s})$ как конкатенацию двух двоичных векторов.

Исходными данными этого процесса являются ключ подписи d и подписываемое сообщение M, а выходным результатом - цифровая подпись w.

Проверка цифровой подписи. Для проверки цифровой подписи w под полученным сообщением M необходимо выполнить следующие действия (шаги).

Шаг 1. По полученной подписи w вычислить целые числа r и s. Если выполнены неравенства $0 < r < q$, $0 < s < q$, то перейти к следующему шагу. В противном случае подпись неверна.

Шаг 2. Вычислить хэш-код полученного сообщения M:

$$\bar{h} = h(M) .$$

Шаг 3. Вычислить целое число α, двоичным представлением которого является вектор $\bar{h}$, и определить

$$e \equiv \alpha (\mathrm{mod}\, q) .$$

Если $e = 0$, то определить $e = 1$.

Шаг 4. Вычислить значение

$$v \equiv e^{-1} (\mathrm{mod}\, q).$$

Шаг 5. Вычислить значения

$$z_1 \equiv sv (\mathrm{mod}\, q), \quad z_2 \equiv -rv (\mathrm{mod}\, q).$$

Шаг 6. Вычислить точку эллиптической кривой $C = z_1 P + z_2 Q$ и определить

$$R \equiv x_C (\mathrm{mod}\, q),$$

где x_C - x-координата точки C.

Шаг 7. Если выполнено равенство $R = r$, то подпись принимается, в противном случае подпись неверна.

Исходными данными этого процесса являются подписанное сообщение M, цифровая подпись w и ключ проверки Q, а выходным результатом - свидетельство о достоверности или ошибочности данной подписи.

Внедрение цифровой подписи на базе стандарта ГОСТ Р 34.10-2001 повышает, по сравнению с предшествующей схемой цифровой подписи, уровень защищенности передаваемых сообщений от подделок и искажений. Этот стандарт рекомендуется использовать в новых системах обработки информации различного назначения, а также при модернизации действующих систем.

3.6. Управление криптоключами

Любая криптографическая система основана на использовании криптографических ключей. Под *ключевой информацией* понимают совокупность всех действующих в информационной сети или системе ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации в сети или системе. *Управление ключами* включает реализацию таких функций, как генерация, хранение и распределение ключей. Распределение ключей - самый ответственный процесс в управлении ключами.

При использовании симметричной криптосистемы две вступающие в информационный обмен стороны должны сначала согласовать секретный сессионный ключ, т.е. ключ для шифрования всех сообщений, передаваемых в процессе обмена. Этот ключ должен быть неизвестен всем остальным и должен периодически обновляться одновременно у отправителя и получателя. Процесс согласования сессионного ключа называют также обменом или распределением ключей.

Асимметричная криптосистема предполагает использование двух ключей - открытого и закрытого (секретного). Открытый ключ можно разглашать, а закрытый надо хранить в тайне. При обмене сообщениями необходимо пересылать только открытый ключ, обеспечив подлинность пересылаемого открытого ключа.

К распределению ключей предъявляются следующие требования:

- оперативность и точность распределения;

- конфиденциальность и целостность распределяемых ключей.

Для распределения ключей между пользователями компьютерной сети используются следующие основные способы [1]:

1) использование одного или нескольких центров распределения ключей;

2) прямой обмен ключами между пользователями сети.

Проблемой первого способа является то, что центру распределения ключей известно, кому и какие ключи распределены, и это позволяет читать все сообщения, передаваемые по сети. Возможные злоупотребления могут существенно нарушить безопасность сети. При использовании второго способа проблема состоит в том, чтобы надежно удостовериться в подлинности субъектов сети.

Задача распределения ключей сводится к построению такого протокола распределения ключей, который обеспечивает:

- взаимное подтверждение подлинности участников сеанса;
- подтверждение достоверности сеанса;
- использование минимального числа сообщений при обмене ключами.

Характерным примером реализации первого подхода является система аутентификации и распределения ключей Kerberos [1]. Остановимся подробнее на втором подходе - прямом обмене ключами между пользователями сети.

При использовании для защищенного информационного обмена криптосистемы с симметричным секретным ключом два пользователя, желающие обменяться криптографически защищенной информацией, должны обладать общим секретным ключом. Эти пользователи должны обменяться общим ключом по каналу связи безопасным образом. Если пользователи меняют ключ достаточно часто, то доставка ключа превращается в серьезную проблему.

Для решения этой проблемы можно применить два основных способа:

1) использование асимметричной криптосистемы с открытым ключом для защиты секретного ключа симметричной криптосистемы;

2) использование системы открытого распределения ключей Диффи - Хеллмана.

Реализация первого способа осуществляется в рамках комбинированной криптосистемы с симметричными и асимметричными ключами. При таком подходе симметричная криптосистема применяется для шифрования и передачи исходного открытого текста, а асимметричная криптосистема с открытым ключом применяется для шифрования, передачи и последующего расшифрования только секретного ключа симметричной криптосистемы.

Второй способ безопасного распространения секретных ключей основан на применении алгоритма открытого распределения ключей Диффи - Хеллмана. Этот алгоритм позволяет пользователям обмениваться ключами по незащищенным каналам связи.

3.6.1. Использование комбинированной криптосистемы

Анализ рассмотренных особенностей симметричных и асимметричных криптографических систем показывает, что при совместном использовании эти криптосистемы могут эффективно друг друга дополнять, компенсируя недостатки друг друга.

Действительно, главным достоинством асимметричных криптосистем с открытым ключом является их потенциально высокая безопасность: нет необходимости ни передавать, ни сообщать кому-либо значения секретных ключей, ни убеждаться в их подлинности. Однако быстродействие асимметричных криптосистем с открытым ключом обычно в сотни и более раз меньше быстродействия симметричных криптосистем с секретным ключом.

В свою очередь, быстродействующие симметричные криптосистемы страдают существенным недостатком: обновляемый секретный ключ симметричной криптосистемы должен регулярно передаваться партнерам по информационному обмену и во время этих передач возникает опасность раскрытия секретного ключа.

Совместное использование этих криптосистем позволяет эффективно реализовать такую базовую функцию защиты, как криптографическое закрытие передаваемой информации с целью обеспечения ее конфиденциальности.

Комбинированное применение симметричного и асимметричного шифрования позволяет устранить основные недостатки, присущие обоим методам. Комбинированный (гибридный) метод шифрования позволяет сочетать преимущества высокой секретности, предоставляемые асимметричными криптосистемами с открытым ключом, с преимуществами высокой скорости работы, присущими симметричным криптосистемам с секретным ключом.

Метод комбинированного использования симметричного и асимметричного шифрования заключается в следующем.

Симметричную криптосистему применяют для шифрования исходного открытого текста, а асимметричную криптосистему с открытым ключом применяют только для шифрования секретного ключа симметричной криптосистемы. В результате асимметричная криптосистема с открытым ключом не заменяет, а лишь дополняет симметричную криптосистему с секретным ключом, позволяя повысить в целом

защищенность передаваемой информации. Такой подход иногда называют схемой *электронного «цифрового конверта»*.

Пусть пользователь *A* хочет использовать комбинированный метод шифрования для защищенной передачи сообщения *M* пользователю *B*. Тогда последовательность действий пользователей *A* и *B* будет следующей.

Действия пользователя *A*:

1. Создает (например, генерирует случайным образом) сеансовый секретный ключ K_s, который будет использован в алгоритме симметричного шифрования для зашифровывания конкретного сообщения или цепочки сообщений.
2. Зашифровывает симметричным алгоритмом сообщение *M* на сеансовом секретном ключе K_s.
3. Зашифровывает асимметричным алгоритмом секретный сеансовый ключ K_s на открытом ключе K_B пользователя *B* (получателя сообщения).
4. Передает по открытому каналу связи в адрес пользователя *B* зашифрованное сообщение *M* вместе с зашифрованным сеансовым ключом K_s.

Действия пользователя *A* иллюстрируются схемой шифрования сообщения комбинированным методом (рис.3.22).

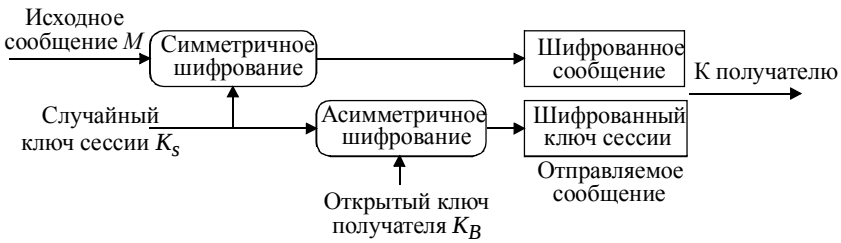

Рис.3.22. Схема шифрования сообщения комбинированным методом

Действия пользователя *B* (при получении электронного «цифрового конверта» - зашифрованного сообщения *M* и зашифрованного сеансового ключа K_s):

5. Расшифровывает асимметричным алгоритмом сеансовый ключ K_s с помощью своего секретного ключа k_B.
6. Расшифровывает симметричным алгоритмом принятое сообщение *M* с помощью полученного сеансового ключа K_s.

Действия пользователя *B* иллюстрируются схемой расшифрования сообщения комбинированным методом (рис.3.23).

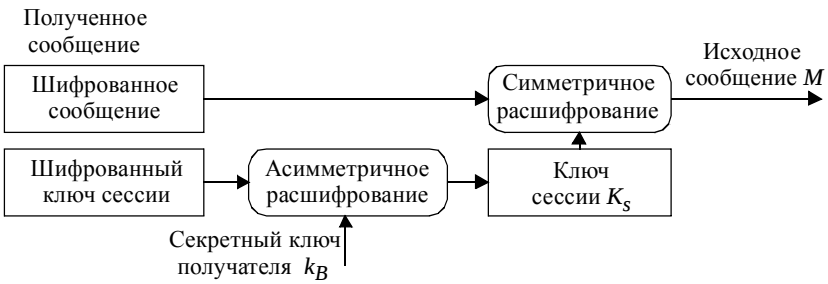

Рис.3.23. Схема расшифрования сообщения комбинированным методом

Полученный электронный «цифровой конверт» может раскрыть только законный получатель - пользователь *B*. Только пользователь *B*, владеющий личным секретным ключом k_B сможет правильно расшифровать секретный сеансовый ключ K_s и затем с помощью этого ключа расшифровать и прочитать полученное сообщение *M*.

При методе «цифрового конверта» недостатки симметричного и асимметричного криптоалгоритмов компенсируются следующим образом:

- проблема распространения ключей симметричного криптоалгоритма устраняется тем, что сеансовый ключ K_s, на котором шифруются собственно сообщения, передается по открытым каналам связи в зашифрованном виде; для зашифрования ключа K_s используется асимметричный криптоалгоритм;
- проблемы медленной скорости асимметричного шифрования в данном случае практически не возникает, поскольку асимметричным криптоалгоритмом шифруется только короткий ключ K_s, а все данные шифруются быстрым симметричным криптоалгоритмом.

В результате получают быстрое шифрование в сочетании с удобным распределением ключей.

С целью защиты от разглашения секретных ключей симметричного шифрования любой из сторон обмена, когда требуется реализовать протоколы взаимодействия не доверяющих друг другу сторон,

используется следующий способ взаимодействия. Для каждого сообщения на основе случайных параметров генерируется отдельный секретный ключ симметричного шифрования, который и зашифровывается асимметричной системой для передачи вместе с сообщением, зашифрованным этим ключом. В этом случае разглашение ключа симметричного шифрования не будет иметь смысла, так как для зашифрования следующего сообщения будет использован другой случайный секретный ключ.

При комбинированном методе шифрования применяются криптографические ключи как симметричных, так и асимметричных криптосистем. Очевидно, выбор длин ключей для криптосистемы каждого типа следует осуществлять таким образом, чтобы злоумышленнику было одинаково трудно атаковать любой механизм защиты комбинированной криптосистемы.

В табл.3.3 приведены распространенные длины ключей симметричных и асимметричных криптосистем, для которых трудность атаки полного перебора примерно равна трудности факторизации соответствующих модулей асимметричных криптосистем [11].

Таблица 3.3

Длина ключа (в бит) для симметричных и асимметричных криптосистем при одинаковой их криптостойкости

Симметричная криптосистема	Асимметричная криптосистема
56	384
64	512
80	768
112	1792
128	2304

Если используется короткий сеансовый ключ (например, 56-битовый ключ алгоритма DES), то не имеет значения, насколько велики асимметричные ключи. Злоумышленник будет атаковать не их, а сеансовый ключ.

3.6.2. Метод распределения ключей Диффи - Хеллмана

У. Диффи и М. Хеллман изобрели метод *открытого распределения ключей* в 1976 году. Этот метод позволяет пользователям обмениваться ключами по незащищенным каналам связи. Его безопасность обусловлена трудностью вычисления дискретных логарифмов в конечном поле, в отличие от легкости решения прямой задачи дискретного возведения в степень в том же конечном поле.

Суть метода Диффи - Хеллмана заключается в следующем (рис.3.24).

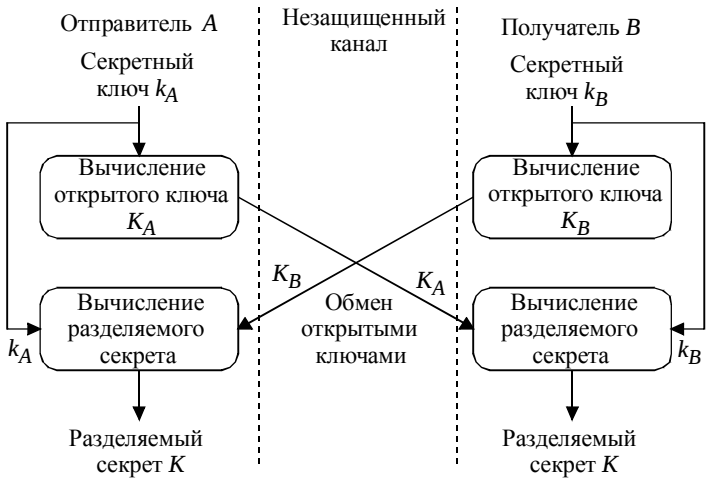

Рис.3.24. Схема открытого распределения ключей Диффи - Хеллмана

Пользователи A и B, участвующие в обмене информацией, генерируют независимо друг от друга свои случайные секретные ключи k_A и k_B (ключи k_A и k_B - случайные большие целые числа, которые хранятся пользователями A и B в секрете).

Затем пользователь A вычисляет на основании своего секретного ключа k_A открытый ключ

$$K_A = g^{k_A} (\mathrm{mod}\ N),$$

одновременно пользователь B вычисляет на основании своего секретного ключа k_B открытый ключ

$$K_B = g^{k_B} \pmod N,$$

где N и g - большие целые простые числа. Арифметические действия выполняются с приведением по модулю N [1]. Числа N и g могут не храниться в секрете. Как правило, эти значения являются общими для всех пользователей сети или системы.

Затем пользователи A и B обмениваются своими открытыми ключами K_A и K_B по незащищенному каналу и используют их для вычисления общего сессионного ключа K (разделяемого секрета):

пользователь A: $K = (K_B)^{k_A} \pmod N = (g^{k_B})^{k_A} \pmod N$,

пользователь B: $K' = (K_A)^{k_B} \pmod N = (g^{k_A})^{k_B} \pmod N$,

при этом $K = K'$, так как $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} \pmod N$.

Таким образом, результатом этих действий оказывается общий сессионный ключ, который является функцией обоих секретных ключей k_A и k_B.

Злоумышленник, перехвативший значения открытых ключей K_A и K_B, не может вычислить сессионный ключ K, потому что он не имеет соответствующих значений секретных ключей k_A и k_B. Благодаря использованию однонаправленной функции операция вычисления открытого ключа необратима, т.е. невозможно по значению открытого ключа абонента вычислить его секретный ключ.

Уникальность метода Диффи - Хеллмана заключается в том, что пара абонентов имеет возможность получить известное только им секретное число, передавая по открытой сети открытые ключи. После этого абоненты могут приступить к защите передаваемой информации уже известным проверенным способом - применяя симметричное шифрование с использованием полученного разделяемого секрета.

Схема Диффи - Хеллмана дает возможность шифровать данные при каждом сеансе связи на новых ключах. Это позволяет не хранить секреты на дискетах или других носителях. Не следует забывать, что любое хранение секретов повышает вероятность попадания их в руки конкурентов или противника.

Схема Диффи - Хеллмана позволяет реализовать *метод комплексной защиты конфиденциальности и аутентичности передаваемых данных*. Эта схема предоставляет пользователям возможность сформировать и использовать одни и те же ключи для выполнения цифровой подписи и симметричного шифрования передаваемых данных.

Для одновременной защиты целостности и конфиденциальности данных целесообразно применять шифрование и электронную цифровую подпись в комплексе. Промежуточные результаты работы схемы Диффи - Хеллмана могут быть использованы в качестве исходных данных для реализации метода комплексной защиты целостности и конфиденциальности передаваемых данных.

Действительно, согласно данному алгоритму пользователи A и B сначала генерируют свои секретные ключи k_A и k_B и вычисляют свои открытые ключи K_A и K_B. Затем абоненты A и B используют эти промежуточные результаты для одновременного вычисления общего разделяемого секретный ключ K, который может использоваться для симметричного шифрования данных.

Метод комплексной защиты конфиденциальности и аутентичности передаваемых данных работает по следующей схеме:

- абонент A подписывает сообщение M с помощью своего секретного ключа k_A, используя стандартный алгоритм цифровой подписи;
- абонент A вычисляет совместно разделяемый секретный ключ K по алгоритму Диффи - Хеллмана из своего секретного ключа k_A и открытого ключа K_B абонента B;
- абонент A зашифровывает сообщение M на полученном совместно разделяемом секретном ключе K, используя согласованный с партнером по обмену алгоритм симметричного шифрования;
- абонент B при получении зашифрованного сообщения M вычисляет по алгоритму Диффи - Хеллмана совместно разделяемый секретный ключ K из своего секретного ключа k_B и открытого ключа K_A абонента A;
- абонент B расшифровывает полученное сообщение M на ключе K;
- абонент B проверяет подпись расшифрованного сообщения M с помощью открытого ключа абонента K_A.

На основе схемы Диффи - Хеллмана функционируют протоколы управления криптоключами SKIP (Simple Key management for Internet Protocols) и IKE (Internet Key Exchange), применяемые при построении защищенных виртуальных сетей VPN на сетевом уровне.

3.6.3. Протокол вычисления ключа парной связи ECKEP

В протоколе вычисления ключа эллиптической кривой ECKEP (Elliptic Curve Key Establishment Protocol) определение параметров системы и генерация ключей аналогичны алгоритму асимметричного шифрования ECES.

Предположим, что общий ключ вычисляется пользователями A и B.

Пользователь A имеет секретный ключ a и открытый ключ $Q_A = aP = (x_A, y_A)$. Аналогично пользователь B имеет секретный ключ b и открытый ключ $Q_B = bP = (x_B, y_B)$.

Вычисление ключа парной связи проводится в четыре этапа.

Этап 1. Действия пользователя A:

- выбирается случайное целое число k_A, $1 \le k_A \le n - 1$;
- вычисляется точка $R_A = k_A P$;
- вычисляется точка $(x_1, y_1) = k_A Q_B$;
- вычисляется $s_A = k_A + a\, x_A\, x_1 \bmod n$;
- R_A отправляется пользователю B.

Этап 2. Действия пользователя B:

- выбирается случайное целое число k_B, $1 \le k_B \le n - 1$;
- вычисляется точка $R_B = k_B P$;
- вычисляется точка $(x_2, y_2) = k_B Q_A$;
- вычисляется $s_B = k_B + b\, x_B\, x_2 \bmod n$;
- R_B отправляется пользователю A.

Этап 3. Действия пользователя A:

- вычисляется $(x_2, y_2) = a\, R_B$;
- вычисляется ключ парной связи $K = s_A (R_B + x_B\, x_2\, Q_B)$;

Этап 4. Действия пользователя B:

- вычисляется $(x_1, y_1) = b\, R_A$;
- вычисляется ключ парной связи $K = s_B (R_A + x_A\, x_1\, Q_A)$, что эквивалентно значению $s_A (R_B + x_B\, x_2\, Q_B)$.

Важным достоинством схемы распределения ключей Диффи -Хеллмана и протокола вычисления ключа парной связи ECKEP является то, что они позволяют обойтись без защищенного канала для передачи ключей. Однако необходимо иметь гарантию того, что пользователь A получил открытый ключ именно от пользователя B и наоборот. Эта проблема решается с помощью сертификатов открытых ключей, создаваемых и распространяемых центрами сертификации CA (Certification Authority) в рамках инфраструктуры управления открытыми ключами PKI (Public Key Infrastructure) [1].

3.7. Инфраструктура управления открытыми ключами PKI

Исторически в задачи любого центра управления информационной безопасностью всегда входил набор задач по управлению ключами, используемыми различными средствами защиты информации (СЗИ). В этот набор входят выдача, обновление, отмена и распространение ключей.

В случае использования симметричной криптографии задача распространения секретных ключей представляла наиболее сложную проблему, поскольку:

- необходимо для N пользователей распространять в защищенном режиме $N(N-1)/2$ ключей, что при N порядка несколько сотен может стать очень обременительной задачей;
- система распространения ключей получается сложной (много ключей и закрытый канал распространения), что приводит к появлению уязвимых мест.

Асимметричная криптография позволяет обойти эту проблему, предложив к использованию только N секретных ключей. При этом у каждого пользователя только один секретный ключ и один открытый, полученный по специальному алгоритму из секретного.

Из открытого ключа практически невозможно получить секретный, поэтому открытый ключ можно распространять открытым способом всем участникам взаимодействия. На основании своего закрытого ключа и открытого ключа своего партнера по взаимодействию любой участник может выполнять любые криптографические операции: электронная цифровая подпись, расчет разделяемого секрета, защита конфиденциальности и целостности сообщения.

В результате решаются две главные проблемы симметричной криптографии:

- перегруженность количеством ключей - их теперь всего N;
- сложность распространения - их можно распространять открыто.

Однако у этой технологии есть один недостаток - подверженность атаке «человек в середине» (man-in-the-middle), когда атакующий злоумышленник расположен между участниками взаимодействия. В этом случае появляется риск подмены передаваемых открытых ключей.

Инфраструктура управления открытыми ключами PKI позволяет преодолеть этот недостаток и обеспечить эффективную защиту от атаки «человек в середине».

3.7.1. Принципы функционирования PKI

Инфраструктура открытых ключей PKI (Public Key Infrastructure) предназначена для надежного функционирования корпоративных информационных систем и позволяет как внутренним, так и внешним пользователям безопасно обмениваться информацией с помощью цепочки доверительных отношений. Инфраструктура открытых ключей PKI основывается на цифровых сертификатах, которые действуют

подобно электронным паспортам, связывающим индивидуальный секретный ключ пользователя с его открытым ключом.

Защита от атаки «человек в середине». При осуществлении атаки «человек в середине» атакующий может незаметно подменить передаваемые по открытому каналу открытые ключи законных участников взаимодействия на свой открытый ключ, создать разделяемые секреты с каждым из законных участников и затем перехватывать и расшифровывать все их сообщения.

Поясним на примере действия атакующего злоумышленника (рис.3.25).

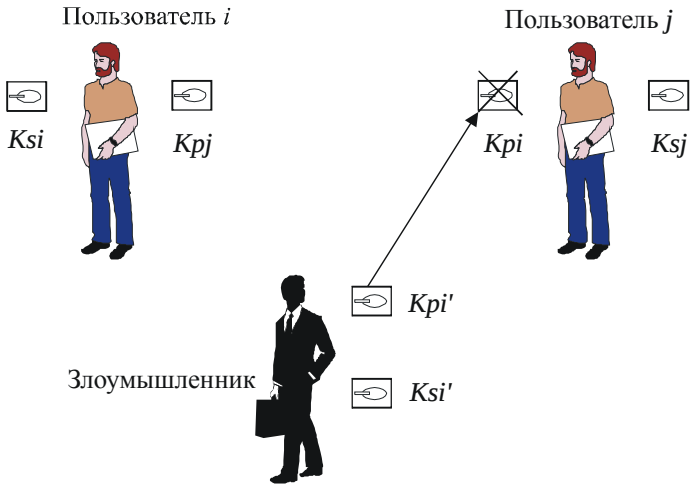

Рис.3.25. Подмена открытого ключа

Предположим, есть два пользователя *i* и *j*, каждый из которых имеет по паре ключей, при этом у пользователя *j* есть открытый ключ *Kpi* для проверки ЭЦП пользователя *i*. Далее предположим, что злоумышленник может перехватить этот ключ *Kpi* в процессе его передачи от пользователя *i* пользователю *j* или получить доступ к этому ключу, хранящемуся у пользователя *j*. В любом случае злоумышленник считает из ключа его реквизиты (например, фамилию владельца, место работы и т.д.) и создаст свою пару ключей - *Ksi'* и *Kpi'*, в которые запишет известные ему реквизиты пользователя *i*. Затем он подменит посланный пользователю *j* открытый ключ *Kpi* своим фальшивым открытым ключом *Kpi'*, имеющим реквизиты пользователя *i*.

Любое сообщение злоумышленник будет подписывать своим секретным ключом *Ksi'* (причем для пользователя *j* эта подпись выглядит так, как если бы она была поставлена пользователем *i*). Подпись такого сообщения, проверяемая этим пользователем *j*, будет верна, поскольку ему был послан фальшивый ключ *Kpi'*, парный столь же фальшивому ключу *Ksi'*.

Подмена открытого ключа раскроется только после того, как настоящий пользователь *i* пошлет пользователю *j* сообщение, подписанное истинным ключом *Ksi*. Но ситуация может находиться под контролем злоумышленника достаточно долго, тем более что он вполне может заранее оценить необходимое время сеансов связи, проанализировав интенсивность документооборота между пользователями *i* и *j*, а также рассчитать время, в течение которого подмена ключа не будет обнаружена. Проблема также существенно усугубляется, если злоумышленник имеет техническую возможность перехватывать сообщения, посылаемые пользователем *i* пользователю *j*.

Описанная угроза подмены открытых ключей успешно устраняется путем использования сертификатов открытых ключей.

Сертификаты открытых ключей. Сертификаты открытых ключей играют важную роль в криптографии открытых ключей. Основное назначение сертификата открытого ключа - сделать доступным и достоверным открытый ключ пользователя.

В основу формирования сертификатов открытых ключей положены принципы строгой аутентификации, рекомендованные стандартом X.509 и базирующиеся на свойствах криптосистем с открытым ключом.

Криптосистемы с открытым ключом предполагают наличие у пользователя парных ключей - секретного и открытого (общедоступного). Каждый пользователь идентифицируется с помощью своего секретного ключа. С помощью парного открытого ключа любой другой пользователь имеет возможность определить, является ли его партнер по связи подлинным владельцем секретного ключа.

Процедура, позволяющая каждому пользователю устанавливать однозначное и достоверное соответствие между открытым ключом и его владельцем, обеспечивается с помощью механизма сертификации открытых ключей.

Степень достоверности факта установления подлинности (аутентификации) пользователя зависит от надежности хранения секретного ключа и надежности источника поставки открытых ключей пользователей.

Чтобы пользователь мог доверять процессу аутентификации, он должен извлекать открытый ключ другого пользователя из надежного источника, которому он доверяет.

Таким источником согласно стандарту X.509 является *Центр сертификации CA (Certification Authority).* Центр сертификации называют также УЦ - *Удостоверяющий центр;* этот термин используется, в частности, в отечественном «Законе об ЭЦП» [14].

Центр сертификации CA является *доверенной третьей стороной*, обеспечивающей аутентификацию открытых ключей, содержащихся в сертификатах. CA имеет собственную пару ключей (открытый/секретный), где секретный ключ CA используется для подписывания сертификатов, а открытый ключ CA публикуется и используется пользователями для проверки подлинности открытого ключа, содержащегося в сертификате.

Сертификация открытого ключа - это подтверждение подлинности открытого ключа и хранимой совместно с ним служебной информации, в частности, о принадлежности ключа. Сертификация ключа выполняется путем вычисления ЭЦП сертифицируемого ключа и служебной информации с помощью специального секретного ключа-сертификата, доступного только Центру сертификации CA. Иными словами, сертификация открытого ключа - это подписывание открытого ключа электронной подписью, вычисленной на секретном ключе Центра сертификации.

Открытый ключ совместно с сертифицирующей его ЭЦП часто называют *сертификатом открытого ключа* или просто *сертификатом*.

Открытый ключ сертификационного центра (парный секретному, на котором проводится сертификация других открытых ключей) используется для проверки целостности сертифицированных открытых ключей. Его обычно называют *ключом-сертификато*м.

Центр сертификации CA формирует сертификат открытого ключа пользователя путем заверения цифровой подписью CA определенного набора данных.

В соответствии с форматом X.509 в этот набор данных включаются:

- период действия открытого ключа, состоящий из двух дат: начала и конца периода;
- номер и серия ключа;
- уникальное имя пользователя;
- информация об открытом ключе пользователя: идентификатор алгоритма, для которого предназначен данный ключ, и собственно открытый ключ;
- ЭЦП и информация, используемая при проведении процедуры проверки ЭЦП (например, идентификатор алгоритма генерации ЭЦП);
- уникальное имя сертификационного центра.

Таким образом, цифровой сертификат содержит три главные составляющие:

- информацию о пользователе - владельце сертификата;
- открытый ключ пользователя;
- сертифицирующую ЭЦП двух предыдущих составляющих, вычисленную на секретном ключе CA.

Сертификат открытого ключа обладает следующими свойствами:

- каждый пользователь, имеющий доступ к открытому ключу Центра сертификации CA, может извлечь открытый ключ, включенный в сертификат;
- ни одна сторона, помимо Центра сертификации, не может изменить сертификат так, чтобы это не было обнаружено (сертификаты нельзя подделать).

Так как сертификаты не могут быть подделаны, то их можно опубликовать, поместив в общедоступный справочник и не предпринимая специальных усилий по защите этих сертификатов.

Создание сертификата открытого ключа начинается с создания пары ключей (открытый/секретный).

Процедура генерации ключей может осуществляться двумя способами.

1. CA создает пару ключей. Открытый ключ заносится в сертификат, а парный ему секретный ключ передается пользователю с обеспечением аутентификации пользователя и конфиденциальности передачи ключа.

2. Пользователь сам создает пару ключей. Секретный ключ сохраняется у пользователя, а открытый ключ передается по защищенному каналу в CA.

Каждый пользователь может быть владельцем одного или нескольких сертификатов, сформированных сертификационным центром CA пользователя. Пользователь может владеть сертификатами, полученными из нескольких разных сертификационных центров.

3.7.2. Логическая структура и компоненты PKI

Инфраструктура открытых ключей PKI (Public Key Infrastructure) - это набор программных агентов и правил, предназначенных для управления ключами, политикой безопасности и собственно обменом защищенными сообщениями [1, 7].

Основными задачами PKI являются:

- поддержка жизненного цикла цифровых ключей и сертификатов (т.е. генерация ключей, создание и подпись сертификатов, их распределение и пр.);
- регистрация фактов компрометации и публикация «черных» списков отозванных сертификатов;

- поддержка процессов идентификации и аутентификации пользователей таким образом, чтобы сократить по возможности время допуска каждого пользователя в систему;
- реализация механизма интеграции (основанного на PKI) существующих приложений и всех компонентов подсистемы безопасности;
- предоставление возможности использования единственного «токена» безопасности, единообразного для всех пользователей и приложений, содержащего все необходимые ключевые компоненты и сертификаты.

Токен безопасности - это индивидуальное средство безопасности, определяющее все права и окружение пользователя в системе, например USB-ключ или смарт-карта.

Приложение, требующее систему управления ключами, должно взаимодействовать с системой PKI в целом ряде точек (передача сертификата на подпись, получение сертификата и «черного» списка при установлении взаимодействия и т.п.). Очевидно, что это взаимодействие с чужой по отношению к данному приложению системой может осуществляться только при условии полной поддержки международных стандартов, которым удовлетворяет большинство современных PKI-систем (например, Baltimore, Entrust, Verisign).

Для предоставления удаленного доступа мобильным пользователям центр управления должен допускать подключение компьютеров, IP-адрес которых ему заранее неизвестен. Участники информационного обмена опознаются по их криптографическим сертификатам. Так как криптографический сертификат пользователя является электронным паспортом, он, как и любой паспорт, должен соответствовать определенным стандартам. В криптографии это стандарт X.509.

Концепция инфраструктуры открытых ключей PKI подразумевает, что все сертификаты конкретной PKI (своя PKI может быть у любой организации или организационной единицы) организованы в иерархическую структуру. Пример иерархии сертификатов двух PKI показан на рис.3.26.

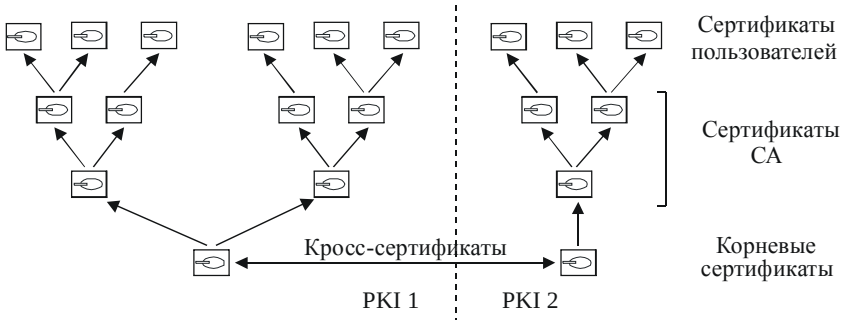

Рис.3.26. Иерархическая структура сертификатов

Иерархическая схема PKI предусматривает существование четырех типов сертификатов.

1. *Сертификат конечного пользователя* (описанный выше).

2. *Сертификат CA*. Должен быть доступен для проверки ЭЦП сертификата конечного пользователя и подписан секретным ключом CA верхнего уровня, причем эта ЭЦП также должна проверяться, для чего должен быть доступен сертификат CA верхнего уровня и т.д.

3. *Самоподписанный сертификат*. Является *корневым* для всей PKI и доверенным по определению. Если в результате проверки цепочки сертификатов CA выяснится, что один из них подписан корневым секретным ключом, тогда процесс проверки ЭЦП сертификатов заканчивается.

4. *Кросс-сертификат*. Кросс-сертификаты позволяют расширить действие конкретной PKI путем взаимоподписания корневых сертификатов двух разных PKI.

Процедура проверки ЭЦП электронного документа происходит в системе PKI следующим образом. Сначала проверяется ЭЦП конкретного документа, а затем ЭЦП сертификата, с помощью которого проверялась предыдущая ЭЦП. Последняя проверка повторяется в цикле до тех пор, пока цепочка сертификатов не приведет к корневому.

ЭЦП документа признается верной лишь в том случае, если верна не только она, но и все проверяемые в данном процессе ЭЦП сертификатов. При обнаружении неверной ЭЦП любого из сертификатов неверными считаются все ЭЦП, проверенные на предыдущих шагах.

Заметим, что корневых сертификатов может быть несколько: каждая организация (или организационная единица) вправе устанавливать свои корневые сертификаты (один или несколько). Стандартом предусмотрено и наличие корневого сертификата для всего сообщества пользователей Интернета.

Логическая структура и основные компоненты инфраструктуры управления открытыми ключами PKI приведены на рис.3.27.

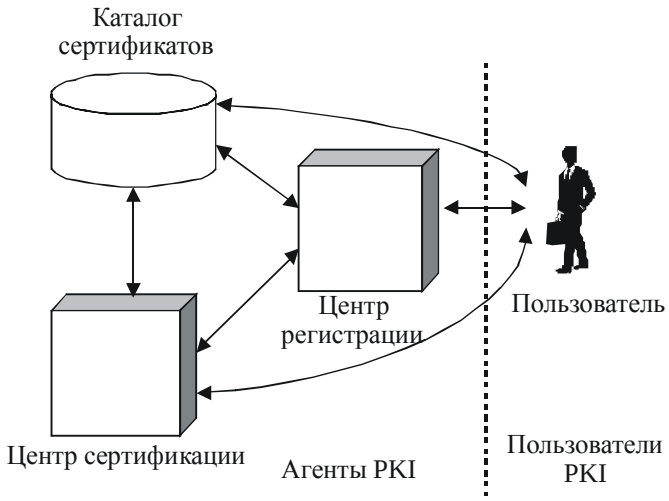

Рис.3.27. Структура PKI

Компоненты этой структуры имеют следующее назначение.

- *Каталог сертификатов* - общедоступное хранилище сертификатов пользователей. Доступ к сертификатам осуществляется обычно по стандартизованному протоколу доступа к каталогам LDAP (Lightweight Directory Access Protocol).
- *Центр регистрации* RA (Registration Authority) - организационная единица, назначение которой - регистрация пользователей системы.
- *Пользователь* - владелец какого-либо сертификата (такой пользователь подлежит регистрации) или любой пользователь, запрашивающий сертификат, хранящийся в каталоге сертификатов.
- *Центр сертификации* CA (Certification Authority) - организационная единица, назначение которой - сертификация открытых ключей пользователей (здесь из открытого ключа получается сертификат формата X.509) и их опубликование в каталоге сертификатов.

Общая схема работы Центра сертификации CA выглядит следующим образом:

- CA генерирует собственные ключи и формирует сертификаты CA, предназначенные для проверки сертификатов пользователей;
- пользователи формируют запросы на сертификацию и доставляют их CA тем или иным способом;
- CA на основе запросов пользователей формирует сертификаты пользователей;
- CA формирует и периодически обновляет списки отмененных сертификатов CRL (Certificate Revocation List);
- сертификаты пользователей, сертификаты CA и списки отмены CRL публикуются CA (рассылаются пользователям либо помещаются в общедоступный справочник).

Функции, выполняемые PKI в целом, можно условно разделить на несколько групп:

- функции управления сертификатами;
- функции управления ключами;
- дополнительные функции (службы).

Кратко рассмотрим эти основные группы функций. В состав *функций управления сертификатами* входят:

- *регистрация пользователей* - «пользователем» может быть физический пользователь, прикладная программа, сетевое устройство и пр.;
- *сертификация открытых ключей* - по существу, процесс сертификации состоит в «связывании» имени пользователя и открытого ключа. CA подписывает сертификаты пользователей и CA более нижнего уровня;
- *сохранение закрытого ключа CA* - это главная болевая точка системы. Компрометация закрытого ключа CA разрушает всю систему;
- *содержание базы сертификатов и их распределение* - все сертификаты пользователей и промежуточных CA (кроме CA самого верхнего уровня!) обычно «выкладываются» на общедоступный сервер - Сервер сертификатов;
- *обновление сертификата* - процесс активизируется в случае истечения срока действия сертификата и состоит в передаче нового сертификата для открытого ключа пользователя;
- *обновление ключей* - при генерации новой пары ключей пользователем либо третьей стороной необходима генерация нового сертификата;
- *отзыв сертификата* - этот процесс возможен, например, при компрометации ключей, изменении имени, прекращении доступа и пр.;

- *определение статуса отзыва сертификата* - пользователь проверяет наличие сертификата в каталоге открытых ключей PKD (Public Key Directory) и в списке отзыва сертификатов CRL (Certificate Revocation List).

Функции управления ключами делятся на следующие основные подгруппы:

- генерация ключей;
- распределение ключей.

В состав группы *дополнительных функций (служб)* входят:

- взаимная сертификация (кросс-сертификация в различных CA);
- проверка открытого ключа с целью убедиться в соответствии открытого ключа арифметическим требованиям для таких ключей;
- проверка сертификата по просьбе пользователя;
- служба архивирования и др.

В состав системы управления инфраструктурой открытых ключей могут входить дополнительные компоненты:

- модули интеграции - программные агенты для прикладных и клиентских систем, программные интерфейсы к сетевым приложениям и Web-сервисам;
- средства хранения ключевой информации и сертификатов пользователя; чаще всего в качестве таких средств выступают аппаратные токены, смарт-карты, USB-ключи.

Интеграция компонентов инфраструктуры открытых ключей со службой каталога позволяет автоматизировать множество задач, связанных с управлением PKI:

- автоматическое создание сертификатов для объектов каталога, управляемое политиками;
- автоматическая публикация списков отозванных сертификатов и сертификатов УЦ.

Кроме того, служба каталога может служить доверенным источником информации о сертификатах других участниках криптографического обмена.

Физически система управления инфраструктурой открытых ключей может состоять из нескольких уровней:

- корневой узел в составе удостоверяющего центра, хранилища сертификатов (служба каталогов) и средств администрирования;
- периферийный узел, включающий центр регистрации, используется при географической распределенности подразделений организации и большом количестве пользователей;
- клиентские станции с необходимыми программными компонентами.

Система управления инфраструктурой открытых ключей и ее компоненты являются основой для создания ряда подсистем комплексной системы обеспечения безопасности организации.

Подсистема управления жизненным циклом отчуждаемых ключевых носителей - подсистема, предназначенная для управления и учета аппаратных средств аутентификации пользователей (USB-ключей и смарт-карт) в масштабах предприятия. Эта подсистема является связующим звеном между пользователями, средствами аутентификации, приложениями информационной безопасности и корпоративной политикой безопасности.

Подсистема генерации ключей шифрования и ЭЦП используется для создания систем юридически значимой электронной цифровой подписи в системах электронного документооборота (в соответствии с Федеральным законом РФ об электронной цифровой подписи № 1-ФЗ от 10.01.2002), реализации систем однократной и многофакторной аутентификации при доступе к автоматизированным информационным системам.

Подсистема безопасного хранения и управления ключевой информацией реализует функции:

- контроля целостности электронных документов;
- контроля целостности публичных информационных ресурсов;
- проверки подлинности взаимодействующих программных компонентов и конфиденциальности передаваемых данных при информационном взаимодействии;
- обеспечения безопасности и разграничения доступа при взаимодействии субъектов автоматизированных информационных систем.

Подсистема защищенного проставления меток времени формирует штампы времени в электронном документообороте, что позволяет создавать доказательство факта существования документа на определенный момент времени.

Инфраструктуру открытых ключей PKI поддерживает ряд приложений и стандартов, к ним можно отнести следующие:

- операционные системы Linux, FreeBSD, HP-UX, Microsoft Windows, Novell Netware, Sun Solaris, в которые встроены средства, поддерживающие сертификаты открытых ключей;
- системы управления базами данных, в частности Oracle, DB2, Informix, Sybase, которые поддерживают механизмы аутентификации пользователей на основе сертификатов открытых ключей;

- средства организации виртуальных защищенных сетей VPN, реализуемые на основе протокола IPSec, в частности телекоммуникационное оборудование компаний Cisco Systems, Nortel Network, а также специализированное программное обеспечение;
- системы электронного документооборота, например Lotus Notes, Microsoft Exchange, а также почтовые системы, поддерживающие стандарт защищенного почтового обмена S/M1ME;
- службы каталогов Microsoft Active Directory, Novell NDS, Netscape iPlanet;
- системы доступа к Web-ресурсам, реализуемые на основе стандарта SSL;
- системы аутентификации пользователей, например система SecurId компании RSA.

В свою очередь, инфраструктура открытых ключей PKI может интегрировать перечисленные функциональные области. В результате можно создавать комплексную систему информационной безопасности путем интеграции инфраструктуры открытых ключей в информационную систему компании и использования единых стандартов и сертификатов открытых ключей.

3.7.3. Инфраструктура открытых ключей на базе продуктов Microsoft

Схема инфраструктуры открытых ключей на базе продуктов Microsoft Active Directory и Microsoft Certification Authority приведена на рис.3.28.

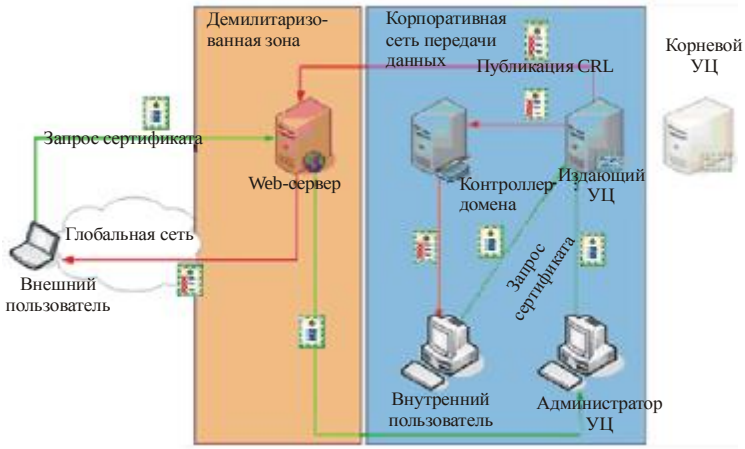

Рис.3.28. Схема инфраструктуры открытых ключей на базе продуктов Microsoft Active Directory и Microsoft Certification Authority

Удостоверяющие центры (УЦ) образуют в приведенном решении двухуровневую иерархию.

Изолированный корневой удостоверяющий центр физически отключен от сети. Этот удостоверяющий центр издает сертификаты только для нижестоящих УЦ. Применение изолированного корневого УЦ позволяет уменьшить риск компрометации всей инфраструктуры открытых ключей в случае успешной атаки на УЦ.

Издающий удостоверяющий центр в данном решении интегрирован в среду MS Active Directory, что позволяет ему автоматически публиковать списки отозванных сертификатов в службе каталога, а также автоматически обслуживать клиентов Active Directory.

Публикация списков отозванных сертификатов производится как в службу каталога, так и на корпоративный Web-сервер (для внешних клиентов, не имеющих доступ к службе каталога организации).

Вопросы для самоконтроля

1. Что такое криптография?
2. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема.
3. В чем состоит коренное различие симметричных и асимметричных криптосистем?
4. Охарактеризуйте четыре основных режима работы блочного алгоритма.
5. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.
6. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?
7. Сформулируйте концепцию криптосистемы с открытым ключом?

8. Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций.

9. Каковы особенности однонаправленных функций с «потайным ходом»?

10. На чем основывается надежность криптоалгоритма шифрования RSA?

11. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.

12. Опишите отечественный стандарт цифровой подписи, укажите его преимущества по сравнению с алгоритмом цифровой подписи DSA.

13. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш-функция?

14. Каким образом комбинированный метод шифрования позволяет сочетать достоинства асимметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.

15. Опишите работу алгоритма Диффи - Хэллмана. Укажите достоинства этого алгоритма.

16. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование инфраструктуры PKI.

Глава 4. Идентификация, аутентификация и управление доступом

Доверие, оказываемое вероломному,
дает ему возможность вредить.

Сенека. «Эдип»

Применение открытых каналов передачи данных создает потенциальные возможности для действий злоумышленников (нарушителей). Поэтому одной из важных задач обеспечения информационной безопасности при взаимодействии пользователей является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны. Обычно для решения данной проблемы применяются специальные приемы, дающие возможность проверить подлинность проверяемой стороны.

4.1. Аутентификация, авторизация и администрирование действий пользователей

С каждым зарегистрированным в компьютерной системе субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов, именующие данный субъект. Эту информацию называют *идентификатором* субъекта. Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (законным) пользователем; остальные пользователи относятся к нелегальным пользователям. Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию и аутентификацию.

Идентификация (Identification) - это процедура распознавания пользователя по его идентификатору, присвоенному данному пользователю ранее и занесенному в базу данных в момент его регистрации в качестве легального пользователя системы. Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация (*Authentication)* - процедура проверки подлинности входящего в систему объекта (пользователя, процесса или устройства), предъявившего свой идентификатор. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления пользователю (процессу или устройству) определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя. *Администрирование (Accounting)* - это процесс управления доступом пользователей к ресурсам системы.

Задачи аутентификации, авторизации и администрирования тесно связаны между собой. Для краткости их взаимосвязанное решение называют решением задач AAA. В настоящее время для решения задач идентификации, аутентификации, авторизации и администрирования используют подсистему управления идентификацией и доступом IAM (Identity and Access Management).

Необходимый уровень аутентификации определяется требованиями безопасности, которые установлены в организации. Общедоступные Web-серверы могут разрешить анонимный или гостевой доступ к информации. Финансовые транзакции могут потребовать строгой аутентификации. Примером слабой формы аутентификации может служить использование IP-адреса для определения пользователя. Подмена (spoofing) IP-адреса может легко разрушить этот механизм аутентификации. Надежная аутентификация является тем ключевым фактором, который гарантирует, что только авторизованные пользователи получат доступ к контролируемой информации.

При защите каналов передачи данных должна выполняться *взаимная аутентификация субъектов*, т.е. взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи. Процедура

подтверждения подлинности выполняется обычно в начале сеанса в процессе установления соединения абонентов. Термин «соединение» указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры - обеспечить уверенность, что соединение установлено с законным субъектом и вся информация дойдет до места назначения.

Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от предъявляемых субъектом сущностей процессы аутентификации могут быть разделены на следующие категории:

- *на основе знания чего-либо*. Примерами могут служить пароль, персональный идентификационный код PIN (Personal Identification Number), а также секретные и открытые ключи, знание которых демонстрируется в протоколах типа запрос-ответ;
- *на основе обладания чем-либо*. Обычно это смарт-карты, сертификаты, USB-ключи или USB-токены (token - опознавательный признак, маркер);
- *на основе каких-либо неотъемлемых характеристик*. Эта категория включает методы, базирующиеся на проверке *биометрических характеристик пользователя* (отпечатки пальцев, радужная оболочка и сетчатка глаза, голос, геометрия ладони и др.). В данной категории не используются криптографические методы и средства. Аутентификация на основе биометрических характеристик применяется для контроля доступа в помещения либо к какой-либо технике [1, 14].

Пароль - это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

Персональный идентификационный номер PIN (Personal Identification Number) является испытанным способом аутентификации держателя пластиковой карты и смарт-карты. Секретное значение PIN-кода должно быть известно только держателю карты.

Динамический (одноразовый) пароль - это пароль, который после однократного применения никогда больше не используется. На практике обычно используется регулярно меняющееся значение, которое базируется на постоянном пароле или ключевой фразе.

Система запрос-ответ - одна из сторон инициирует аутентификацию с помощью посылки другой стороне уникального и непредсказуемого значения «запрос», а другая сторона посылает ответ, вычисленный с помощью «запроса» и секрета. Так как обе стороны владеют одним секретом, то первая сторона может проверить правильность ответа второй стороны.

Сертификаты и цифровые подписи - если для аутентификации используются сертификаты, то требуется применение цифровых подписей на этих сертификатах. Сертификаты выдаются ответственным лицом в организации пользователя, сервером сертификатов или внешней доверенной организацией. В рамках Интернета появился ряд коммерческих инфраструктур управления открытыми ключами PKI (Public Key Infrastructure) для распространения сертификатов открытых ключей. Пользователи могут получить сертификаты различных уровней.

Процессы аутентификации можно также классифицировать по уровню обеспечиваемой безопасности [1, 14]. В соответствии с данным подходом процессы аутентификации разделяются на следующие типы:

- простая аутентификация, использующая пароли;
- строгая аутентификация, использующая многофакторные проверки и криптографические методы;
- биометрическая аутентификация пользователей.

С точки зрения безопасности каждый из перечисленных типов способствует решению своих специфических задач, поэтому процессы и протоколы аутентификации активно используются на практике.

Основными атаками на протоколы аутентификации являются:

- «маскарад» *(impersonation)* - пользователь пытается выдать себя за другого с целью получения полномочий и возможности действий от лица другого пользователя;
- *подмена стороны аутентификационного обмена (interleaving attack)* - злоумышленник в ходе данной атаки участвует в процессе аутентификационного обмена между двумя сторонами с целью модификации проходящего через него трафика;
- *повторная передача (replay attack)* - заключается в повторной передаче аутентификационных данных каким-либо пользователем;
- *принудительная задержка (forced delay)* - злоумышленник перехватывает некоторую информацию и передает ее спустя некоторое время;
- *атака с выборкой текста (chosen-text attack)* - злоумышленник перехватывает аутентификационный трафик и пытается получить информацию о долговременных криптографических ключах.

Для предотвращения таких атак при построении протоколов аутентификации применяются следующие приемы:

- использование механизмов типа запрос-ответ, меток времени, случайных чисел, идентификаторов, цифровых подписей;

- привязка результата аутентификации к последующим действиям пользователей в рамках системы. Примером подобного подхода может служить осуществление в процессе аутентификации обмена секретными сеансовыми ключами, которые используются при дальнейшем взаимодействии пользователей;
- периодическое выполнение процедур аутентификации в рамках уже установленного сеанса связи и т.п.

Механизм запроса-ответа состоит в следующем. Если пользователь *A* хочет быть уверенным, что сообщения, получаемые им от пользователя *B*, не являются ложными, он включает в посылаемое для *B* сообщение непредсказуемый элемент - запрос *X* (например, некоторое случайное число). При ответе пользователь *B* должен выполнить над этим элементом некоторую операцию (например, вычислить некоторую функцию *f*(*X*)). Это невозможно осуществить заранее, так как пользователю *B* неизвестно, какое случайное число *X* придет в запросе. Получив ответ с результатом действий *B*, пользователь *A* может быть уверен, что *B* - подлинный. Недостаток этого метода - возможность установления закономерности между запросом и ответом.

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить, насколько «устарело» пришедшее сообщение, и решить не принимать его, поскольку оно может быть ложным. При использовании отметок времени возникает проблема *допустимого временного интервала задержки* для подтверждения подлинности сеанса. Ведь сообщение с «временным штемпелем», в принципе, не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

4.2. Методы аутентификации, использующие пароли

Одной из распространенных схем аутентификации является *простая аутентификация*, которая основана на применении традиционных многоразовых паролей с одновременным согласованием средств его использования и обработки. Пока в некоторых защищенных виртуальных сетях VPN (Virtual Private Network) доступ клиента к серверу разрешается по паролю. Однако все чаще применяются более эффективные средства аутентификации, например программные и аппаратные системы аутентификации на основе одноразовых паролей, системы аутентификации на основе смарт-карт, USB-токенов и цифровых сертификатов.

4.2.1. Аутентификация на основе многоразовых паролей

В современных операционных системах предусматривается централизованная служба аутентификации, которая выполняется одним из серверов сети и использует для своей работы базу данных. В этой базе данных хранятся учетные данные о пользователях сети. В эти учетные данные наряду с другой информацией включены идентификатор (login) и пароль (password) пользователя [11].

Процедуру аутентификации пользователя с использованием многоразового пароля можно представить следующим образом. При попытке логического входа пользователя в сеть он набирает на клавиатуре своего компьютера свои идентификатор и пароль. Эти данные поступают для обработки на сервер аутентификации. В базе данных учетных записей пользователей, хранящейся на сервере аутентификации, по идентификатору пользователя находится соответствующая запись, из нее извлекается эталонное значение пароля и сравнивается с тем паролем, который ввел пользователь. Если введенная пользователем пара login/password совпала с эталонной, то аутентификация прошла успешно, пользователь получает легальный статус и получает те права и ресурсы сети, которые определены для его статуса системой авторизации.

В схеме простой аутентификации передача пароля и идентификатора пользователя может проводиться следующими способами [1]:

- в незашифрованном виде, например согласно протоколу парольной аутентификации PAP (Password Authentication Protocol) пароли передаются по линии связи в открытой незащищенной форме;
- в защищенном виде - все передаваемые данные (идентификатор и пароль пользователя, случайное число и метки времени) защищены посредством шифрования или однонаправленной функции.

Вариант аутентификации с передачей пароля пользователя в незашифрованном виде не гарантирует даже минимального уровня безопасности, так как подвержен многочисленным атакам и легко компрометируется.

Схема аутентификации с передачей пароля в защищенном виде показана на рис.4.1.

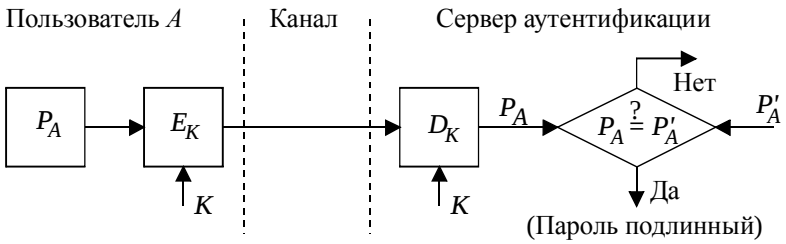

Рис.4.1. Простая аутентификация с использованием пароля

Чтобы защитить пароль, его шифруют перед пересылкой по незащищенному каналу. Для этого в схему включены средства шифрования E_K и расшифрования D_K, управляемые разделяемым секретным ключом K. Проверка подлинности пользователя основана на сравнении присланного пользователем пароля P_A и исходного значения P'_A, хранящегося в сервере аутентификации. Если значения P_A и P'_A совпадают, то пароль P_A считается подлинным, а пользователь A - законным.

Схемы организации простой аутентификации отличаются не только методами передачи паролей, но и видами их хранения и проверки. Для обеспечения надежной защиты операционной системы пароль каждого пользователя должен быть известен только этому пользователю и никому другому, в том числе и администраторам системы. Пароли пользователей не должны храниться в операционной системе в открытом виде.

С точки зрения безопасности предпочтительным является метод передачи и хранения паролей с использованием односторонних функций. Обычно для шифрования паролей в списке пользователей используют одну из известных криптографически стойких *хэш-функций*. В списке пользователей хранится не сам пароль, а *образ пароля*, являющийся результатом применения к паролю хэш-функции.

Однонаправленность хэш-функции не позволяет восстановить пароль по образу пароля, но позволяет, вычислив хэш-функцию, получить образ введенного пользователем пароля и таким образом проверить правильность введенного пароля. В простейшем случае в качестве хэш-функции используется результат шифрования некоторой константы на пароле.

Например, односторонняя функция $h(.)$ может быть определена следующим образом:

$$h(P) = E_P\,(ID),$$

где P - пароль пользователя; ID - идентификатор пользователя; E_P - процедура шифрования, выполняемая с использованием пароля P в качестве ключа.

Такие функции удобны, если длина пароля и ключа одинаковы. В этом случае проверка подлинности пользователя A с помощью пароля P_A состоит из пересылки серверу аутентификации отображения $h(P_A)$ и сравнения его с предварительно вычисленным и хранимым в базе данных сервера аутентификации эквивалентом $h'(P_A)$. Если отображения $h(P_A)$ и $h'(P_A)$ равны, то считается, что пользователь успешно прошел аутентификацию.

Системы простой аутентификации на основе многоразовых паролей не обладают достаточной безопасностью, поскольку в них выбор аутентифицирующей информации происходит из относительно небольшого множества слов. Такие пароли можно перехватить, разгадать, подсмотреть или просто украсть. Срок действия многоразового пароля должен быть определен в политике безопасности организации, и такие пароли должны регулярно изменяться. Выбирать пароли нужно так, чтобы они были трудны для угадывания и не присутствовали в словаре.

4.2.2. Аутентификация на основе одноразовых паролей

Как уже отмечалось, схемы аутентификации, основанные на традиционных многоразовых паролях, не обладают достаточной безопасностью. Более надежными являются процедуры аутентификации на основе одноразовых паролей OTP (One Time Password).

Суть схемы одноразовых паролей - использование различных паролей при каждом новом запросе на предоставление доступа. Одноразовый динамический пароль действителен только для одного входа в систему, затем его действие истекает. Даже если кто-то перехватил его, пароль окажется бесполезен. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от угроз извне.

Одноразовые пароли генерируются с помощью OTP-токена. Для этого используется секретный ключ пользователя, размещенный как внутри OTP-токена, так и на сервере аутентификации. Примером алгоритма формирования одноразовых паролей является HOTP, разработанный Международной ассоциацией OATH (Open AuTHentication Group). Алгоритм использует в качестве входных значений секретный ключ K и текущее значение счетчика генераций N, который увеличивается при каждой новой генерации пароля.

Алгоритм HOTP сначала вычисляет значение согласно алгоритму хеширования HMAC-SHA-1, а затем выполняет операцию выделения (Truncate) из полученного 160-битового значения 6 цифр, являющихся одноразовым паролем:

HOTP (K, N) = Truncate (HMAC-SHA-1(K, N)), где K - секретный ключ и N - счетчик генераций.

Чтобы получить доступ к необходимым ресурсам, пользователь должен ввести пароль, созданный с помощью OTP-токена. Этот пароль сравнивается со значением, сгенерированным на сервере аутентификации, после чего выносится решение о предоставлении пользователю доступа. Преимуществом такого подхода является то, что пользователю не требуется соединять токен с компьютером. Недостатком OTP-токенов является ограниченное время жизни этих устройств (три-четыре года), так как автономность работы предполагает использование батарейки. Обычно системы аутентификации с одноразовыми паролями используются для проверки удаленных пользователей.

4.3. Строгая аутентификация

Идея строгой аутентификации заключается в следующем. Проверяемая (доказывающая) сторона доказывает свою подлинность проверяющей стороне, демонстрируя знание некоторого секрета [11]. Этот секрет может быть предварительно распределен безопасным способом между сторонами аутентификационного обмена.

4.3.1. Основные понятия

В соответствии с рекомендациями стандарта X.509 различают процедуры строгой аутентификации следующих типов:

- односторонняя аутентификация;
- двусторонняя аутентификация;
- трехсторонняя аутентификация.

Односторонняя аутентификация предусматривает обмен информацией только в одном направлении. Данный тип аутентификации позволяет:

- подтвердить подлинность только одной стороны информационного обмена;
- обнаружить нарушение целостности передаваемой информации;
- обнаружить проведение атаки типа повтор передачи;
- гарантировать, что передаваемыми аутентификационными данными может воспользоваться только проверяющая сторона.

Двусторонняя аутентификация по сравнению с односторонней содержит дополнительный ответ проверяющей стороны доказывающей стороне, который должен убедить ее, что связь устанавливается именно с той стороной, которой были предназначены аутентификационные данные.

Трехсторонняя аутентификация содержит дополнительную передачу данных от доказывающей стороны проверяющей.

Следует отметить, что данная классификация достаточно условна. Отмеченные особенности носят в большей степени теоретический характер. На практике набор используемых приемов и средств зависит непосредственно от конкретных условий реализации процесса аутентификации.

Как уже отмечалось, процессы строгой аутентификации могут быть реализованы на основе многофакторных проверок и на основе использования криптографических методов.

4.3.2. Двухфакторная аутентификация

Строгая аутентификация может быть реализована на основе двух- или трехфакторного процесса проверки, по результатам которого пользователю может быть предоставлен доступ к запрашиваемым ресурсам.

В первом случае пользователь должен доказать, что он знает пароль или PIN-код и имеет определенный персональный идентификатор (смарт-карту или USB-ключ). Во втором случае пользователь предъявляет еще один тип идентификационных данных, например биометрические данные. На практике более широкое применение находит двухфакторная аутентификация.

Применение средств многофакторной аутентификации снижает роль паролей, и в этом проявляется еще одно преимущество строгой аппаратной аутентификации, так как, по некоторым оценкам, пользователям приходится помнить до 15 различных паролей для доступа к учетным записям. Из-за информационной перегруженности сотрудники, чтобы не забыть пароли, записывают их на бумаге, что снижает уровень безопасности из-за компрометации пароля. Использование усиленной или двухфакторной аутентификации позволяет не только снизить риски ИТ-безопасности, но и оптимизировать внутренние процессы компании вследствие уменьшения прямых финансовых потерь.

Использование для двухфакторной аутентификации пользователей внешних носителей информации (смарт-карт и USB-токенов) позволяет заметно повысить защищенность системы. В отличие от паролей, владелец быстро узнает о краже внешнего носителя информации и может сразу принять необходимые меры для предотвращения ее негативных последствий.

Аутентификацию на основе смарт-карт и USB-токенов сложнее обойти, так как используется уникальный физический объект, которым должен обладать человек, чтобы войти в систему. Двухфакторная аутентификация на основе смарт-карт и USB-токенов намного надежнее многоразовых паролей.

В отличие от доступа пользователей к системе с предъявлением имени пользователя и пароля, системы двухфакторной аутентификации изменяют порядок аутентификации, взамен предъявления пароля пользователь должен предъявить физический носитель - смарт-карту или токен, содержащий сертификат и секретный ключ пользователя. При этом пользователь должен предъявить не только данный носитель секретного ключа, но и ввести PIN-код доступа к носителю, причем ни секретный ключ, ни PIN-код ни в каком виде по корпоративной сети не передаются. Отсутствие передачи секретного ключа и PIN-кода через сеть значительно повышает безопасность процесса аутентификации.

Применение смарт-карт. Смарт-карты - это интеллектуальные пластиковые карты стандартного размера кредитной карты, которые помимо энергонезависимой памяти содержат микропроцессор, способный выполнять криптографические преобразования информации.

По способу обмена данными с устройством ввода-вывода смарт-карты подразделяются на контактные и бесконтактные.

Контактный способ обмена данными подразумевает непосредственное соприкосновение контактов контактной смарт-карты с устройством ввода-вывода.

Бесконтактный (дистанционный) способ обмена данными не требует четкого позиционирования бесконтактной смарт-карты и устройства ввода-вывода. Чтение или запись данных происходит при поднесении бесконтактной смарт-карты на определенное расстояние к устройству ввода-вывода.

Основным компонентом контактных и бесконтактных смарт-карт являются одна или более встроенных интегральных микросхем (чипов), которые могут представлять собой микросхемы памяти, микросхемы с жесткой логикой и микропроцессоры (процессоры). В настоящее время наибольшей функциональностью и степенью защищенности обладают смарт-карты с микропроцессором.

Основу внутренней структуры микропроцессорной смарт-карты составляет чип, в состав которого входят центральный процессор, специализированный криптографический процессор (опционально), оперативная память (RAM), постоянная память (ROM), электрически перепрограммируемая постоянная память только для чтения EEPROM, датчик случайных чисел, таймеры, последовательный коммуникационный порт (рис.4.2).

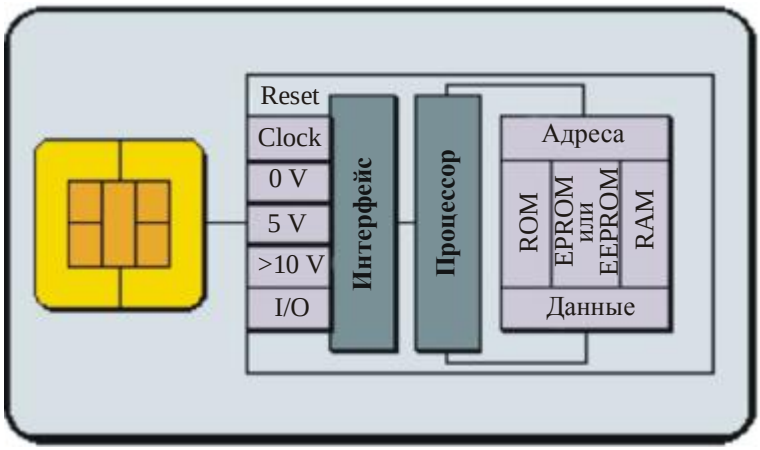

Рис.4.2. Структура контактной микропроцессорной смарт-карты

Оперативная память RAM используется для временного хранения данных, например результатов вычислений, произведенных процессором. Ее емкость составляет несколько килобайтов. В постоянной памяти ROM хранятся команды, исполняемые процессором, и другие неизменяемые данные. Информация в ROM записывается при производстве карты. Емкость памяти может составлять десятки килобайтов.

В смарт-картах используются два типа памяти PROM: однократно программируемая память EPROM и более распространенная многократно программируемая память EEPROM. В ней хранятся пользовательские данные, которые могут считываться, записываться и модифицироваться, и конфиденциальные данные (например, криптографические ключи), не доступные для прикладных программ. Емкость памяти составляет десятки и сотни килобайтов.

Центральный процессор смарт-карты (обычно это RISC-процессор) обеспечивает реализацию разнообразных процедур обработки данных, контроль доступа к памяти и управление ходом выполнения вычислительного процесса.

На специализированный процессор возлагается реализация различных процедур, необходимых для повышения защищенности системы идентификации и аутентификации (СИА), в том числе:

- генерация криптографических ключей;

- реализация криптографических алгоритмов (ГОСТ 28147-89, DES, 3DES, AES, RSA, SHA-1);
- выполнение операций с электронной цифровой подписью (генерация и проверка);
- выполнение операций с PIN-кодом и др.

В ПЗУ хранится исполняемый код процессора, оперативная память используется в качестве рабочей, EEPROM необходима для хранения изменяемых данных владельца карты.

В отличие от контактных смарт-карт, в состав бесконтактных смарт-карт на базе стандарта MIFARE Standard дополнительно входит радиочастотный модуль со встроенной антенной, необходимой для связи со считывателем и питания микросхемы.

Бесконтактные смарт-карты функционируют на частоте 13,56 МГц и разделяются на два класса, которые базируются на международных стандартах ISO/IEC 14443 и ISO/IEC 15693.

Для использования смарт-карт в компьютерных системах необходимо считывающее устройство (или считыватель) смарт-карт. Устройства чтения смарт-карт могут подключаться к компьютеру посредством последовательного порта, слота PCMCIA или USB.

Смарт-карты осуществляют хранение сертификатов пользователей и ключевого материала в самом устройстве, поэтому секретный ключ пользователя не попадает во враждебную внешнюю среду. Для проведения успешной аутентификации требуется вставить смарт-карту в считывающее устройство и ввести пароль (PIN-код). Операционная система считывает идентификатор пользователя и соответствующий ему ключ.

Для хранения и использования закрытого ключа используются разные подходы. Наиболее простой из них - применение устройства аутентификации в качестве защищенного носителя аутентификационной информации: при необходимости карта экспортирует закрытый ключ и криптографические операции осуществляются на рабочей станции. Этот подход является не самым совершенным с точки зрения безопасности, зато относительно легко реализуемым и предъявляющим невысокие требования к устройству аутентификации.

Два других подхода более безопасны, поскольку предполагают выполнение устройством аутентификации криптографических операций: пользователь генерирует ключи на рабочей станции и сохраняет их в памяти устройства; пользователь генерирует ключи при помощи устройства. В обоих случаях после того как закрытый ключ сохранен, его нельзя извлечь из устройства и получить любым другим способом.

При *генерации ключевой пары вне устройства* пользователь может сделать резервную копию закрытого ключа. Если устройство выйдет из строя, будет потеряно, повреждено или уничтожено, пользователь сможет сохранить тот же закрытый ключ в памяти нового устройства. Это необходимо, если пользователю требуется расшифровать какие-либо данные или сообщения, зашифрованные с помощью соответствующего открытого ключа. Однако при этом закрытый ключ пользователя подвергается риску быть похищенным, что означает его компрометацию.

При *генерации ключевой пары с помощью устройства* закрытый ключ не появляется в открытом виде и нет риска его похищения. Единственный способ использования закрытого ключа - это обладание устройством аутентификации. Являясь наиболее безопасным, это решение выдвигает высокие требования к возможностям самого устройства: оно должно обладать функциональностью генерации ключей и осуществления криптографических преобразований. Это решение также предполагает, что закрытый ключ не может быть восстановлен в случае выхода устройства из строя. Подобным образом способны работать микропроцессорные смарт-карты, например Athena ASECard Crypto, Schlumberger Cryptoflex и др.

Следует отметить, что интеллектуальные смарт-карты способны самостоятельно проверять правильность пароля на доступ к ключевой информации, и при аутентификации пользователя с использованием интеллектуальной карты проверку пароля на доступ к карте может производить не операционная система, а сама карта [14]. Интеллектуальная карта может быть запрограммирована на стирание хранимой информации после превышения максимально допустимого количества неправильных попыток ввода пароля, что не позволяет подбирать пароль без частого копирования карты, а это весьма дорого.

Смарт-карты оптимальны для использования в инфраструктуре открытых ключей PKI, так как осуществляют безопасное хранение ключевого материала и сертификатов пользователей в самом устройстве. Достоинством смарт-карты является удобство ее хранения (например, ее можно держать в бумажнике вместе с другими карточками).

Недостатками смарт-карт являются низкая мобильность, поскольку для работы с ними требуется считывающее устройство, а также ограниченный срок эксплуатации из-за неустойчивости смарт-карты к механическим повреждениям и относительно высокая стоимость считывателей смарт-карт.

Применение USB-токенов. USB-токены являются преемниками контактных смарт-карт. Поэтому структуры и функциональность USB-токенов и смарт-карт практически идентичны.

В состав USB-токенов могут входить:

- микропроцессор - управление и обработка данных;
- криптографический процессор - реализация алгоритмов ГОСТ 28147-89, DES, 3DES, RSA, DSA, MD5, SHA-1 и других криптографических преобразований;
- USB-контроллер - обеспечение интерфейса с USB-портом компьютера;

- оперативная память RAM - хранение изменяемых данных;
- защищенная память EEPROM - хранение ключей шифрования, паролей, сертификатов и других важных данных;
- постоянная память ROM - хранение команд и констант.

Конструктивно USB-ключи выпускаются в виде брелоков (рис.4.3),

Рис.4.3. Идентификатор eToken R2

которые легко размещаются на связке с обычными ключами. Брелоки выпускаются в цветных корпусах и снабжаются световыми индикаторами работы. Каждый идентификатор имеет прошиваемый при изготовлении собственный уникальный 32/64-разрядный серийный номер.

USB-токены со встроенным чипом обладают всеми преимуществами смарт-карт, связанными с безопасным хранением конфиденциальных сведений и осуществлением криптографических операций прямо внутри токена, но лишены их основного недостатка, т.е. не требуют дорогостоящего аппаратного считывателя. USB-токен подключается к USB-порту непосредственно или с помощью соединительного кабеля, поскольку USB является стандартным портом для подключения периферийных устройств.

Процесс двухфакторной аутентификации с использованием USB-токенов проходит в два этапа: пользователь подключает это небольшое устройство в USB-порт компьютера и вводит PIN-код.

Поддержка спецификаций PC/SC позволяет без труда переходить от смарт-карт к USB-ключам и встраивать их как в существующие приложения, так и в новые.

Многофункциональность токенов обеспечивает широкие возможности их применения - от строгой аутентификации и организации безопасного локального или удаленного входа в вычислительную сеть до построения на основе токенов систем юридически важного электронного документооборота, шифрования файлов, организации защищенных каналов передачи данных, управления правами пользователя, осуществления безопасных транзакций и др.

Достоинствами USB-токенов являются малые размеры и удобство хранения, отсутствие аппаратного считывателя, простота подсоединения к USB-порту, высокая мобильность, так как USB-порты имеются на каждой рабочей станции и на любом ноутбуке. «Слабым» местом USB-токенов является ограниченный ресурс их USB-разъемов. Например, для идентификаторов семейства eToken гарантированное число подключений составляет 5000 раз. К недостаткам можно также отнести относительно высокую стоимость и слабую механическую защищенность брелока.

Особенности использования PIN-кода. Наиболее распространенным методом аутентификации держателя смарт-карты или USB-токена является ввод секретного числа, которое обычно называют *PIN-кодом (Personal Identification Number - персональный идентификационный код)* или иногда CHV (CardHolder Verification). Защита PIN-кода является критичной для безопасности всей системы. Карты могут быть потеряны, украдены или подделаны. В таких случаях единственной контрмерой против несанкционированного доступа остается секретное значение PIN-кода. Вот почему открытая форма PIN должна быть известна только законному держателю карты. Очевидно, что значение PIN нужно держать в секрете в течение всего срока действия карты и токена.

С одной стороны, длина PIN-кода должна быть достаточно большой, чтобы минимизировать вероятность определения правильного PIN-кода методом проб и ошибок. С другой стороны, длина PIN-кода должна быть достаточно короткой, чтобы дать возможность держателям карт запомнить его значение. Согласно рекомендации стандарта ISO 9564-1, PIN-код должен содержать от четырех до двенадцати буквенно-цифровых символов. Однако в большинстве случаев ввод нецифровых символов технически невозможен, поскольку доступна только цифровая клавиатура. Поэтому обычно PIN-код представляет собой четырехразрядное число, каждая цифра которого может принимать значение от 0 до 9.

PIN-код вводится с помощью клавиатуры терминала или компьютера и затем отправляется на смарт-карту. Смарт-карта сравнивает полученное значение PIN-кода с эталонным значением, хранимым в карте, и отправляет результат сравнения на терминал. Ввод PIN-кода относится к мерам безопасности, особенно для финансовых транзакций, и, следовательно, требования к клавиатуре часто определяются в этой прикладной области. PIN-клавиатуры имеют все признаки модуля безопасности, и они шифруют PIN-код сразу при его вводе. Это обеспечивает надежную защиту против проникновения в клавиатуру для того, чтобы перехватить PIN-код в то время, когда он вводится.

Рекомендуется устанавливать ограничения на число неверных попыток ввода PIN-кода. Когда число обнаруженных неверных попыток достигает заданного предела, процесс ввода должен быть заблокирован, препятствуя дальнейшим попыткам аутентификации. Допустимое число неверных попыток устанавливают в диапазоне от 1 до 255. Метод, используемый для разблокирования процесса ввода, должен быть защищен независимым механизмом аутентификации.

Для *генерации PIN-кода* смарт-карты используются генератор случайных чисел и алгоритм, который преобразует случайное число в PIN-код необходимой длины. Затем можно использовать таблицу известных тривиальных комбинаций, чтобы распознать и отбросить значение PIN-кода, совпадающее с одной из таких комбинаций. Наконец, этот PIN-код записывается в смарт-карту в виде соответствующей криптограммы. Вычисленное значение PIN-кода передается также держателю смарт-карты, пользуясь защищенным каналом.

Главное требование безопасности использования PIN-кода состоит в том, что значение PIN-кода должно запоминаться держателем карты и не должно храниться в любой читаемой форме. Но память людей несовершенна, и часто они забывают значения своих PIN-кодов. Поэтому эмитенты карт должны иметь специальные процедуры для таких случаев. Эмитент может реализовать один из следующих подходов. Первый основан на восстановлении забытого клиентом значения PIN-кода и отправке его обратно владельцу карты. При втором подходе просто генерируется новое значение PIN-кода.

При идентификации клиента по значению PIN-кода и предъявленной карте используются два основных способа проверки PIN-кода: неалгоритмический и алгоритмический [1].

Неалгоритмический способ проверки PIN-кода не требует применения специальных алгоритмов. Проверка PIN-кода осуществляется путем непосредственного сравнения введенного клиентом PIN-кода со значениями, хранимыми в базе данных. Обычно база данных со значениями PIN-кодов клиентов шифруется методом прозрачного шифрования, чтобы повысить ее защищенность, не усложняя процесса сравнения.

Алгоритмический способ проверки PIN-кода заключается в том, что введенный клиентом PIN-код преобразуют по определенному алгоритму с использованием секретного ключа и затем сравнивают со значением PIN-кода, хранящимся в определенной форме на карте. Достоинства этого метода проверки следующие:

- отсутствие копии PIN-кода на главном компьютере исключает его раскрытие обслуживающим персоналом;
- отсутствие передачи PIN-кода между банкоматом или кассиром-автоматом и главным компьютером банка исключает его перехват злоумышленником или навязывание результатов сравнения.

4.3.3. Криптографические протоколы строгой аутентификации

При строгой аутентификации, реализуемой в криптографических протоколах, проверяемая сторона доказывает свою подлинность проверяющей стороне, демонстрируя знание некоторого секрета с использованием криптографических методов и средств.

Существенным является тот факт, что доказывающая сторона демонстрирует только знание секрета, но сам секрет в ходе аутентификационного обмена не раскрывается. Это обеспечивается посредством ответов доказывающей стороны на различные запросы проверяющей стороны. При этом результирующий запрос зависит только от пользовательского секрета и начального запроса, который обычно представляет произвольно выбранное в начале протокола большое число.

В большинстве случаев строгая аутентификация заключается в том, что каждый пользователь аутентифицируется по признаку владения своим секретным ключом. Иначе говоря, пользователь имеет возможность определить, владеет ли его партнер по связи надлежащим секретным ключом и может ли он использовать этот ключ для подтверждения того, что он действительно является подлинным партнером по информационному обмену.

Необходимо также учитывать, что проведение строгой аутентификации требует обязательного согласования сторонами используемых криптографических алгоритмов и ряда дополнительных параметров [11]. Прежде чем перейти к рассмотрению протоколов строгой аутентификации, следует остановиться на назначении и возможностях так называемых одноразовых параметров, используемых в протоколах аутентификации. Эти одноразовые параметры иногда называют *nonces*. По определению, *nonce* - это величина, используемая для одной и той же цели не более одного раза. Среди используемых на сегодняшний день одноразовых параметров следует выделить: случайные числа, метки времени и номера последовательностей.

Одноразовые параметры позволяют избежать повтора передачи, подмены стороны аутентификационного обмена и атаки с выбором открытого текста. При помощи одноразовых параметров можно обеспечить уникальность, однозначность и временные гарантии передаваемых сообщений. Различные типы одноразовых параметров могут употребляться как отдельно, так и дополнять друг друга.

В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации можно разделить на следующие группы:

- строгой аутентификации на основе симметричных алгоритмов шифрования;
- строгой аутентификации на основе однонаправленных ключевых хэш-функций;
- строгой аутентификации на основе асимметричных алгоритмов шифрования;
- строгой аутентификации на основе алгоритмов электронной цифровой подписи.

Рассмотрим подробнее протоколы строгой аутентификации на основе симметричных алгоритмов шифрования. Для работы протоколов аутентификации, построенных на основе симметричных алгоритмов, необходимо, чтобы проверяющий и доказывающий с самого начала имели один и тот же секретный ключ. Для закрытых систем с небольшим количеством пользователей каждая пара пользователей может заранее разделить его между собой. В больших распределенных системах, применяющих технологию симметричного шифрования, часто используются протоколы аутентификации с участием доверенного сервера, с которым каждая сторона разделяет знание ключа. Такой сервер распределяет сеансовые ключи для каждой пары пользователей всякий раз, когда один из них запрашивает аутентификацию другого.

Ниже приводятся два примера протоколов строгой аутентификации на основе симметричных алгоритмов шифрования, специфицированных в ISO/IEC 9798-2. Эти протоколы предполагают предварительное распределение разделяемых секретных ключей.

Рассмотрим следующие варианты аутентификации:

- односторонняя с использованием случайных чисел;
- двусторонняя с использованием случайных чисел.

В каждом из этих случаев пользователь доказывает свою подлинность, демонстрируя знание секретного ключа, так как производит расшифровывание запросов с помощью этого секретного ключа.

Введем следующие обозначения:

r_A - случайное число, сгенерированное участником A;

r_B - случайное число, сгенерированное участником B;

E_K - симметричное шифрование на ключе K (ключ K должен быть предварительно распределен между A и B).

1. Односторонняя аутентификация, основанная на использовании случайных чисел:

$$A \leftarrow B: r_B$$

$$A \rightarrow B: E_K(r_B, B).$$

Участник B отправляет участнику A случайное число r_B. Участник A шифрует сообщение, состоящее из полученного числа r_B и идентификатора B, и отправляет зашифрованное сообщение участнику B. Участник B расшифровывает полученное сообщение и сравнивает случайное число, содержащееся в сообщении, с тем, которое он послал участнику A. Дополнительно он проверяет имя, указанное в сообщении.

2. Двусторонняя аутентификация, использующая случайные значения:

$$A \leftarrow B: r_B$$

$$A \rightarrow B: E_K(r_A, r_B, B)$$

$$A \leftarrow B: E_K(r_A, r_B).$$

При получении второго сообщения участник B выполняет те же проверки, что и в предыдущем протоколе, и дополнительно расшифровывает случайное число r_A для включения его в третье сообщение для участника A. Третье сообщение, полученное участником A, позволяет ему убедиться на основе проверки значений r_A и r_B, что он имеет дело именно с участником B.

Широко известными представителями протоколов, обеспечивающих аутентификацию пользователей с привлечением в процессе аутентификации третьей стороны, являются протокол распределения секретных ключей Нидхэма и Шредера и протокол Kerberos.

Протоколы аутентификации, представленные выше, могут быть модифицированы путем замены симметричного шифрования на шифрование с помощью односторонней ключевой хэш-функции. Это бывает необходимо, если алгоритмы блочного шифрования недоступны или не отвечают предъявляемым требованиям (например, в случае экспортных ограничений). Своеобразие шифрования с помощью односторонней хэш-функции заключается в том, что оно, по существу, является односторонним, т.е. не сопровождается обратным преобразованием - расшифровыванием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования [14].

4.4. Биометрическая аутентификация пользователя

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, персональный идентификатор, секретный ключ и т.п.). Привычные системы аутентификации не всегда удовлетворяют современным требованиям в области

информационной безопасности, особенно если речь идет об ответственных приложениях (онлайновые финансовые приложения, доступ к удаленным базам данных и т.п.).

В последнее время все большее распространение получает биометрическая аутентификация пользователя, позволяющая уверенно аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения. Использование решений, основанных на биометрической технологии, позволяет в ряде случаев улучшить положение дел в области аутентификации.

Для методов аутентификации, основанных на использовании многоразовых паролей, характерен следующий недостаток - многоразовый пароль может быть скомпрометирован множеством способов. Недостатком методов, связанных с использованием токенов, является возможность потери, кражи, дублирования токенов - носителей критической информации. Биометрические методы, использующие для идентификации уникальные характеристики пользователя, свободны от перечисленных недостатков.

Отметим основные преимущества биометрических методов аутентификации пользователя по сравнению с традиционными:

- высокая степень достоверности аутентификации по биометрическим признакам из-за их уникальности;
- неотделимость биометрических признаков от дееспособной личности;
- трудность фальсификации биометрических признаков.

В качестве биометрических признаков, которые активно используются при аутентификации потенциального пользователя, можно выделить следующие:

- отпечатки пальцев;
- узор радужной оболочки и сетчатки глаз;
- геометрическая форма кисти руки;
- форма и размеры лица;
- особенности голоса.

Рассмотрим типичную схему функционирования биометрической подсистемы аутентификации. При регистрации в системе пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой как контрольный «образец» законного пользователя. Биометрический образец обрабатывается системой для получения информации в виде эталонного идентификатора пользователя (ЭИП) или эталона для проверки. ЭИП представляет собой числовую последовательность, при этом сам образец невозможно восстановить из эталона.

Эталонный идентификатор пользователя ЭИП хранится системой в электронной форме и используется для проверки идентичности каждого, кто выдает себя за соответствующего законного пользователя. Снятая в процессе идентификации характеристика пользователя сравнивается с ЭИП. Поскольку эти два значения (полученное при попытке доступа и ЭИП) полностью никогда не совпадают, то для принятия положительного решения о доступе степень совпадения должна превышать определенную настраиваемую пороговую величину. В зависимости от степени совпадения или несовпадения совокупности предъявленных признаков с ЭИП лицо их предъявившее признается законным пользователем (при совпадении) или нет (при несовпадении).

С точки зрения потребителя, эффективность биометрической аутентификационной системы характеризуется двумя параметрами:

- коэффициентом ошибочных отказов FRR (false-reject rate);
- коэффициентом ошибочных подтверждений FAR (false-alarm rate).

Ошибочный отказ возникает тогда, когда система не подтверждает личность законного пользователя (типичные значения FRR составляют порядка одной ошибки на 100). *Ошибочное подтверждение* происходит в случае подтверждения личности незаконного пользователя (типичные значения FAR составляют порядка одной ошибки на 10 000). Коэффициент ошибочных отказов и коэффициент ошибочных подтверждений связаны друг с другом; каждому коэффициенту ошибочных отказов соответствует определенный коэффициент ошибочных подтверждений.

В совершенной биометрической системе оба параметра ошибки должны быть равны нулю. К сожалению, биометрические системы не идеальны, поэтому приходится чем-то пожертвовать. Обычно системные параметры настраивают так, чтобы добиться требуемого коэффициента ошибочных подтверждений, что определяет соответствующий коэффициент ошибочных отказов.

К настоящему времени разработаны и продолжают совершенствоваться технологии аутентификации по отпечаткам пальцев, радужной оболочке глаза, по форме кисти руки и ладони, по форме и размеру лица, по голосу и «клавиатурному почерку».

Наибольшее число биометрических систем в качестве параметра идентификации использует отпечатки пальцев (дактилоскопические системы). Отпечаток пальца считается одним из наиболее устойчивых идентификационных признаков (не изменяется со временем, при повреждении кожного покрова идентичный папиллярный узор полностью восстанавливается, при сканировании не вызывает дискомфорта у пользователя).

Дактилоскопические системы аутентификации. Одной из основных причин широкого распространения таких систем является наличие больших банков данных по отпечаткам пальцев.

Основными пользователями подобных систем во всем мире являются полиция, различные государственные и некоторые банковские организации.

В общем случае биометрическая технология распознавания отпечатков пальцев заменяет защиту доступа с использованием пароля. Большинство систем используют отпечаток одного пальца, который пользователь предоставляет системе.

Основными элементами дактилоскопической системы аутентификации являются:

- сканер;
- ПО идентификации, формирующее идентификатор пользователя;
- ПО аутентификации, производящее сравнение отсканированного отпечатка пальца с имеющимися в базе данных «паспортами» пользователей.

Дактилоскопическая система аутентификации работает следующим образом. Сначала проводится регистрация пользователя. Как правило, проводится несколько вариантов сканирования в разных положениях пальца на сканере. Понятно, что образцы будут немного отличаться и требуется сформировать некоторый обобщенный образец, «паспорт». Результаты запоминаются в базе данных аутентификации. При аутентификации сравниваются отсканированный отпечаток пальца с «паспортами», хранящимися в базе данных.

Задача формирования «паспорта», так же как и задача распознавания предъявляемого образца, является задачей распознавания образов. Для этого используются различные алгоритмы, являющиеся ноу-хау фирм-производителей подобных устройств.

Сканеры отпечатков пальцев. Многие производители все чаще переходят от дактилоскопического оборудования на базе оптики к продуктам, основанным на интегральных схемах. Продукты на базе интегральных схем имеют значительно меньшие размеры, чем оптические считыватели, и поэтому их проще реализовать в широком спектре периферийных устройств.

Ряд производителей комбинируют биометрические системы со смарт-картами и картами-ключами. Например, в биометрической идентификационной смарт-карте Authentic реализован следующий подход. Образец отпечатка пальца пользователя запоминается в памяти карты в процессе внесения в списки идентификаторов пользователей, устанавливая соответствие между образцом и личным ключом шифрования. Затем, когда пользователь вводит смарт-карту в считыватель и прикладывает палец к сканеру, ключ удостоверяет его личность. Комбинация биометрических устройств и смарт-карт является удачным решением, повышающим надежность процессов аутентификации и авторизации.

Небольшой размер и невысокая цена датчиков отпечатков пальцев на базе интегральных схем превращает их в идеальный для человека интерфейс для систем защиты.

Системы аутентификации по узору радужной оболочки и сетчатки глаз. Такие системы могут быть разделены на два класса:

- использующие рисунок радужной оболочки глаза;
- использующие рисунок кровеносных сосудов сетчатки глаза.

Сетчатка человеческого глаза представляет собой уникальный объект для аутентификации. Рисунок кровеносных сосудов глазного дна отличается даже у близнецов. Поскольку вероятность повторения параметров радужной оболочки и сетчатки глаза имеет порядок 10^{-78}, такие системы являются наиболее надежными среди всех биометрических систем. Такие средства идентификации применяются там, где требуется высокий уровень безопасности (например, в режимных зонах военных и оборонных объектов).

Системы аутентификации по форме ладони. Такие системы используют сканеры формы ладони, обычно устанавливаемые на стенах. Следует отметить, что подавляющее большинство пользователей предпочитают системы этого типа.

Устройства считывания формы ладони создают объемное изображение ладони, измеряя длину пальцев, толщину и площадь поверхности ладони. Например, продукты компании Recognition Systems выполняют более 90 измерений, которые преобразуются в девятиразрядный образец для дальнейших сравнений. Этот образец может быть сохранен локально, на индивидуальном сканере ладони либо в централизованной базе данных. Сканеры формы ладони хорошо подходят для вычислительных сред со строгим режимом безопасности и напряженным трафиком, включая серверные комнаты. Они достаточно точны и обладают довольно низким коэффициентом ошибочного отказа FRR (false rejection rate), т.е. процентом отклоненных законных пользователей.

Системы аутентификации по лицу и голосу. Эти системы являются наиболее доступными из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства. Системы данного класса применяются при удаленной идентификации субъекта доступа в телекоммуникационных сетях.

Технология сканирования черт лица подходит для тех приложений, где прочие биометрические технологии непригодны. В этом случае для идентификации и верификации личности используются особенности глаз, носа и губ. Производители устройств распознавания черт лица используют собственные математические алгоритмы для идентификации пользователей. Следует отметить, что большая часть алгоритмов распознавания черт лица чувствительна к колебаниям в освещении, вызванным изменением интенсивности солнечного света в течение дня. Изменение положения лица также может повлиять на узнаваемость.

Системы аутентификации по голосу экономически выгодны по тем же причинам, что и системы распознавания по чертам лица. В частности, их можно устанавливать с оборудованием (например, микрофонами), поставляемым в стандартной комплектации со многими ПК. Системы аутентификации по голосу при записи образца и в процессе последующей идентификации опираются на такие уникальные для каждого человека особенности голоса, как высота, модуляция и частота звука. Эти показатели определяются физическими характеристиками голосового тракта и уникальны для каждого человека.

Технологии распознавания говорящего имеют некоторые ограничения. Различные люди могут говорить похожими голосами, а голос любого человека может меняться со временем в зависимости от самочувствия, эмоционального состояния и возраста. Поскольку голос сам по себе не обеспечивает достаточной точности, распознавание по голосу следует сочетать с другими биометриками, такими, как распознавание черт лица или отпечатков пальцев.

Биометрическая аутентификация пользователя может играть серьезную роль в *шифровании*. Ахиллесовой пятой многих систем шифрования является проблема безопасного хранения криптографического секретного ключа. Зачастую доступ к ключу длиной 128 бит или даже больше защищен лишь паролем из 6 символов, т.е. 48 бит. Отпечатки пальцев обеспечивают намного более высокий уровень защиты в отличие от пароля, который можно забыть.

4.5. Управление доступом по схеме однократного входа с авторизацией Single Sign-On

Большинство пользователей информационных средств и систем используют компьютеры для доступа к ряду сервисов, будь это несколько локальных приложений или более сложные приложения, которые включают одну или более удаленных систем, к которым машина пользователя подсоединяется через сеть. В целях обеспечения безопасности многие приложения требуют проведения аутентификации пользователя прежде, чем ему дадут доступ к сервисам и данным, предоставляемым приложением.

Конечные пользователи обычно воспринимают такие требования системы безопасности как дополнительную нагрузку, которая заставляет поддерживать и помнить многочисленные входные идентификаторы и пароли и использовать их каждый день по несколько раз, чтобы иметь возможность выполнять свою обычную работу. Довольно типична ситуация, когда один пользователь имеет пять и более таких пользовательских accounts, все на различных платформах с различными правилами для длин паролей, а также с различной частотой их замены. Пользователь должен либо заучивать их все наизусть, либо записывать их в места, где их могут найти неавторизованные пользователи, подвергая тем самым безопасность серьезному риску.

С увеличением числа требующих запоминания паролей возрастает вероятность того, что они будут забываться. Это потребует от администраторов дополнительных усилий по восстановлению паролей. Данную проблему часто называют «проблемой многих входов». Решить ее позволяет схема однократного входа с авторизацией SSO (Single Sign-On).

Управление доступом по схеме однократного входа с авторизацией SSO дает возможность пользователям корпоративной сети при их входе в сеть пройти одну аутентификацию, предъявив только один раз пароль (или иной требуемый аутентификатор), и затем без дополнительной аутентификации получить доступ ко всем авторизованным сетевым ресурсам, которые им нужны для выполнения их работы. Такими сетевыми ресурсами могут быть принтеры, приложения, файлы и другие данные, размещаемые по всему предприятию на серверах различных типов, работающих на базе различных операционных систем. Управление доступом по схеме однократного входа SSO позволяет повысить производительность труда пользователей сети, уменьшить стоимость сетевых операций и улучшить сетевую безопасность.

С функционированием схемы SSO непосредственно связаны процессы аутентификации и авторизации. Большинство подходов SSO централизованно осуществляют аутентификацию пользователя. Авторизацию обычно выполняют на ресурсах целевых объектов, хотя некоторые SSO-решения централизованно осуществляют и авторизацию.

Схему однократного входа SSO поддерживают такие средства, как протокол LDAP (Lightweight Directory Access Protocol), протокол SSL (Secure Sockets Layer), система Kerberos и инфраструктура управления открытыми ключами PKI (Public Key Infrastructure), а также средства интеграции сервисов каталогов и безопасности. Эти средства и технологии образуют вместе фундамент для применения схемы однократного входа SSO.

Существуют решения схемы однократного входа SSO от простых средств до SSO уровня предприятия [1]. Компания Microsoft предоставляет возможности интегрированной и простой в использовании SSO на базе операционной системы Microsoft Windows. Большие приложения, такие, как Lotus Notes/Domino или Netscape Communicator/SuiteSpot, допускают один вход ко всем их прикладным функциям (почта, базы данных дискуссионных форумов, справочники, основанные на сертификатах, логины и др.).

4.5.1. Простая система однократного входа Single Sign-On

Самое простое SSO-решение состоит в том, чтобы автоматизировать процесс предъявления пароля (рис.4.4).

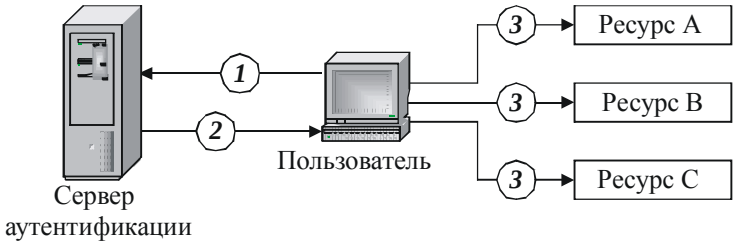

Рис.4.4. Простое SSO-решение - автоматизация входа

При автоматизации процедуры входа выполняются следующие шаги.

Шаг 1. Пользователь предъявляет серверу аутентификации пароль, используя специальное клиентское программное обеспечение на своем персональном компьютере.

Шаг 2. Сервер аутентификации проверяет, к каким ресурсам может получить доступ этот пользователь и отправляет эту информацию обратно на клиентское SSO-приложение совместно с необходимым мандатом входа и scripts для соединения с каждым разрешенным ресурсом**.**

Шаг 3. Клиентское SSO-приложение предоставляет пользователю доступные ресурсы и входит от имени пользователя в выбранные приложения.

Автоматизация процедуры входа позволяет получить простую схему SSO, но при этом еще больше децентрализуется администрирование безопасностью. Ряд поставщиков предлагает дополнительные средства централизованного администрирования безопасностью. Эти средства используют агентов в целевых системах и обеспечивают основанное на ролях (role-based) централизованное администрирование учетных записей пользователей и информации об их полномочиях. В некоторых случаях эти средства администрирования отделены от схемы SSO, в других случаях они интегрированы с SSO.

Продвинутые SSO-решения предоставляют больше контроля над полномочиями пользователя, поддерживаемыми обычно на прикладном уровне. Минимально такие решения включают агентов для общего сервера и сред приложений, которые обеспечивают централизованное, основанное на ролях администрирование полномочий пользователя по нескольким ресурсам. Целевой ресурс доверяет SSO-системе идентифицировать конкретных пользователей и их роли; SSO эффективно доставляет доверенные мандаты к приложению, скрывая от приложения процесс аутентификации.

4.5.2. Системы однократного входа Web SSO

Разработчики первых Web-сайтов были вынуждены создавать свои собственные SSO-решения и столкнулись с рядом трудностей. Однако вскоре разработчики Web SSO получили помощь в виде «cookie» со стороны поставщиков Web-браузеров. Компании Microsoft и Novell - два главных поставщика Web-браузеров - очень рано ввели в своих продуктах поддержку cookie. В качестве cookie могут быть использованы зашифрованные данные пользователя (зашифрованный мандат пользователя). «Cookie» - это часть информации, которую Web-сервер хранит в ПК пользователя с помощью приложения браузера и которую можно использовать при принятии решения о предоставлении пользователю доступа, поэтому «cookie» стали широко распространенным и популярным механизмом для создания Web SSO. Если имя пользователя хранится в cookie в ПК пользователя, серверное приложение может проверить, кем является этот пользователь, не предлагая ему предъявлять пароль снова, независимо от того, на какую страницу сайта переходит этот пользователь.

Проблема однократного входа с авторизацией SSO (Single Sign-On) была успешно решена во Всемирной паутине, поскольку требование Web-сайтом многократного предъявления пароля является просто недопустимым вариантом. Действительно, коммерческий Web-сайт, который потребует от посетителя сайта предъявить пароль несколько раз за сессию, подвергнет суровому испытанию терпение посетителей и быстро растеряет всех своих потенциальных клиентов. В настоящее время схема однократного входа SSO на Web-сайт является практически обязательным сервисом (рис.4.5).

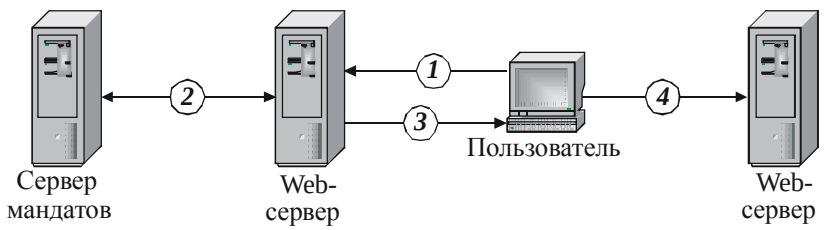

Рис.4.5. Схема Web SSO, основанная на использовании cookie (Cookie-based Web SSO)

Следует отметить, что большинство из продвинутых корпоративных Web-сайтов извлекает свои данные из серверных баз данных.

В схеме Web SSO, основанной на использовании cookie, при реализации процедуры входа выполняются следующие шаги.

Шаг 1. Пользователь, используя специальное клиентское программное обеспечение на своем персональном компьютере, передает на Web-сервер имя пользователя и пароль.

Шаг 2. Агент Web-сервера извлекает мандат пользователя из сервера мандатов (Credentials Server). Web-сервер предоставляет пользователю ресурсы в соответствии с его мандатом.

Шаг 3. Агент Web-сервера сохраняет зашифрованный мандат в качестве cookie на компьютере пользователя.

Шаг 4. Когда пользователь переходит на другую страницу на Web-сайте, которая может быть на другом Web-сервере, этот Web-сервер просто читает мандат пользователя из его cookie.

Вскоре после своего появления cookies стали подвергаться атакам, но поскольку теперь cookies могут передаваться с помощью шифрованной SSL-сессии, эта проблема практически исключена.

На рис.4.6 показана схема Web SSO, не использующая cookies.

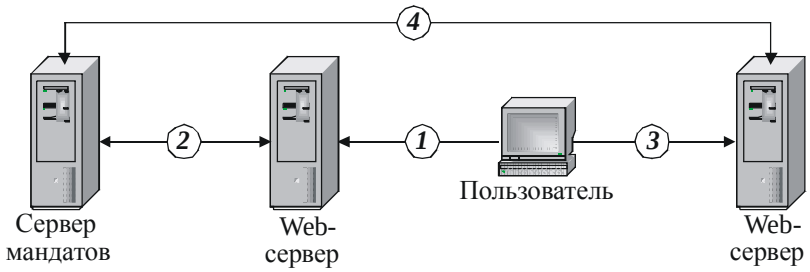

Рис.4.6. Схема Web SSO, не использующая cookies

В схеме Web SSO, не использующей cookies, при реализации процедуры входа выполняются следующие шаги.

Шаг 1. Пользователь передает на Web-сервер имя пользователя и пароль.

Шаг 2. Агент на Web-сервере извлекает мандат пользователя из сервера мандатов (Credentials Server). Web-сервер предоставляет пользователю ресурсы в соответствии с его мандатом.

Шаг 3. Если пользователь пытается получить доступ к защищенным ресурсам на другом Web-сервере, агент на этом Web-сервере должен снова запрашивать мандат пользователя на сервере мандатов.

Коммерческие Web SSO-решения используют ряд подходов. Почти во всех подходах требуется использование агентов, инсталлированных на Web-серверы, которые связываются с отдельным мандатным сервером, чтобы проверить подлинность пользователя. Некоторые варианты также требуют собственного клиентского программного обеспечения. Такой подход может дать более высокий уровень безопасности при использовании технологий аутентификации на основе одноразовых токенов или возможностей PKI.

4.5.3. SSO-продукты уровня предприятия

SSO-продукты уровня предприятия проектируются для больших компаний с гетерогенной распределенной компьютерной средой, состоящей из многих систем и приложений. Схема однократного входа с авторизацией SSO дает возможность пользователям корпоративной сети при входе в сеть пройти одну аутентификацию и затем получить доступ к сетевым ресурсам, которые им нужны для выполнения работы. Такими сетевыми ресурсами могут быть приложения, файлы и другие данные, размещаемые по всему предприятию на серверах различных типов, работающих на базе различных операционных систем.

Характерным представителем SSO-продуктов уровня предприятия является продукт IBM Global Sign-On for Multiplatforms (GSO). Продукт GSO представляет безопасное, простое в использовании решение, позволяющее пользователю получать доступ к сетевым компьютерным ресурсам, используя однократный вход в систему. GSO осуществляет безопасное хранение пользовательских идентификаторов IDs и паролей и обеспечение ими целевых объектов, когда пользователю нужно предъявить пароль при входе. Это освобождает пользователя от необходимости помнить и вводить эти IDs и пароль каждый день для каждого целевого объекта.

На рис.4.7 показана базовая схема ячейки GSO. Ячейка GSO содержит, по крайней мере, сервер GSO и одну рабочую станцию пользователя, называемую также клиентом GSO. В ячейке GSO может быть более одного сервера GSO и множество клиентов.

Пользователь взаимодействует со своей рабочей станцией и некоторыми целевыми объектами (приложениями), которые могут выполняться на этой рабочей станции или на каком-либо другом компьютере, например сервере приложений.

Перед тем как начать работу, пользователь должен войти в свою рабочую станцию. Пользователь предъявляет пароль именно GSO, а не приложению или другим серверам. GSO выполняет аутентификацию, основанную на идентификаторе ID и пароле пользователя (иногда поддерживаемых смарт-картой или

считывателем отпечатков пальцев). Сервер GSO включается в процесс аутентификации для того, чтобы проверить пароль пользователя и извлечь его мандат (credentials).

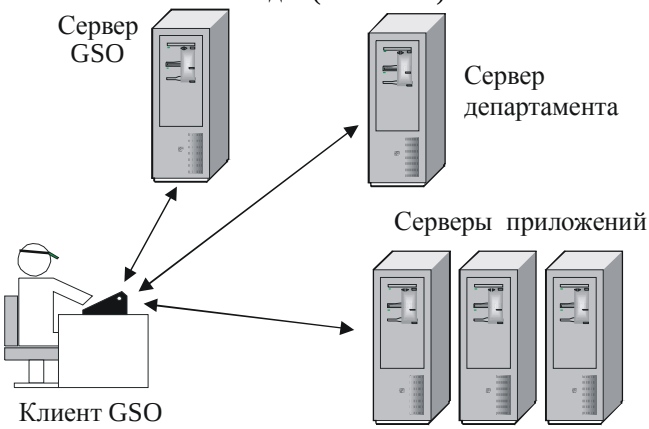

Рис.4.7. Базовые компоненты GSO

Затем GSO будет вводить пользователя в целевые объекты (приложения или сервера), с которыми этот пользователь должен работать. GSO использует для входа пользователя методы, предоставляемые целевыми объектами. В большинстве случаев GSO имитирует вход пользователя, передавая целевому объекту ID и пароль пользователя, как будто вводит их сам пользователь. Важное различие состоит в том, что теперь пользователю не нужно запоминать эти идентификаторы ID и пароли, поскольку заботу о них принимает на себя GSO.

GSO является клиент/серверным приложением. В дополнение к серверу GSO существует программа клиента (сегмент программного кода), выполняемая на рабочей станции пользователя, которая взаимодействует с сервером GSO.

SSO-продукты уровня предприятия обладают следующими достоинствами:

- допускают использование многих целевых платформ со своими собственными механизмами аутентификации;
- безопасно хранят в базах данных учетную информацию пользователей (такую, как идентификатор ID, пароль и некоторую дополнительную информацию) на каждую целевую платформу и каждого пользователя;
- радикально уменьшается доля забываемых паролей, поскольку пароли пользователей хранятся безопасно и надежно;
- используются методы и средства безопасной аутентификации и коммуникации. Чувствительная пользовательская информация хранится и передается по сети только в зашифрованном виде.

Недостатками SSO-продуктов уровня предприятия является их относительно большая стоимость и высокие требования к квалификации обслуживающего персонала.

Вопросы для самоконтроля

1. Дайте определения понятий: идентификация, аутентификация, авторизация, администрирование. Что понимают под решением задач AAA?
2. Какие задачи решает подсистема управления идентификацией и доступом IAM (Identity and Access Management)?
3. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
4. Перечислите основные атаки на протоколы аутентификации.
5. Опишите метод аутентификации на основе многоразовых паролей. Каковы недостатки этого метода?
6. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
7. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.
8. Объясните назначение PIN-кода и особенности его использования.
9. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используются для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?
10. Опишите функциональность и характеристики смарт-карт и USB-токенов.
11. Опишите методы биометрической аутентификации пользователя. Что означают коэффициент ошибочных отказов и коэффициент ошибочных подтверждений?
12. Поясните принцип управления доступом по схеме однократного входа с авторизацией Single Sign-On.

Глава 5. Защита электронного документооборота

Сколь беззащитно наше счастье,
доверенное чужим рукам.
Уильям Хэзлитт

Для современной организации прикладные системы являются эффективным инструментом повышения производительности и качества труда за счет того, что позволяют систематизировать выполнение информационных процессов. Характерным примером прикладной информационной системы является система электронного документооборота.

Системы электронного документооборота играют важную роль в государственном управлении, а также в управлении организациями, имеющими разветвленную сеть подразделений, филиалов и представительств. Чем глубже прикладные информационные системы интегрируются в бизнес организаций, тем сильнее бизнес зависит от надежности этих систем. Нарушение нормального функционирования прикладных систем и корпоративной информационной системы в целом может привести к прямым потерям для организации.

Наблюдающееся в настоящее время увеличение сложности прикладных систем повышает возможность появления уязвимостей в их реализации. Используя эти уязвимости, внешние и внутренние злоумышленники могут нарушить конфиденциальность, целостность и доступность обрабатываемых в прикладных системах данных.

К защите информации в прикладных системах предъявляется ряд законодательных требований. Среди них можно отметить Федеральный закон об информации, информационных технологиях и защите информации, Закон о коммерческой тайне, Закон о персональных данных и др.

Обеспечение безопасности прикладных систем основывается на построении комплексной системы информационной безопасности. Мероприятия по защите информации в прикладных системах должны включать программно-технические средства и организационно-управленческие мероприятия. Программно-технические средства могут быть представлены как средствами инфраструктурного уровня, так и специфичными для заданной прикладной системы средствами.

5.1. Концепция электронного документооборота

С развитием локальных и глобальных сетей все шире используются системы электронного документооборота (СЭД). Такие системы существенно расширяют возможности как коммерческих компаний, так и государственных организаций.

Электронный документооборот - это способ организации работы с документами, при котором основная масса документов организации (предприятия) используется в электронном виде и хранится централизованно.

Система электронного документооборота - компьютерная программа (программное обеспечение, система и т.п.), которая позволяет организовать работу с электронными документами (создание, изменение, поиск), а также взаимодействие между сотрудниками (передачу документов, выдачу заданий, отправку уведомлений и т.п.).

Иногда СЭД называют EDMS (Electronic Document Management Systems - система управления электронными документами).

Системы электронного документооборота относят к классу прикладных систем управления корпоративными информационными ресурсами ECM (Enterprise Content Management) [27].

Под системой ECM понимают набор технологий, инструментов и методов, используемых для сбора, управления, накопления, хранения и доставки информации (контента) всем потребителям внутри организации. Это понятие несколько шире, чем СЭД. Например, для того чтобы стать ECM-системой, СЭД должна содержать средства сканирования документов, гарантировать сохранность документов, поддерживать правила хранения документов и т.д.

По сравнению с бумажным документооборотом электронный документооборот имеет ряд преимуществ:

- *сокращение затрат времени руководителей и сотрудников* - использование СЭД сокращает временные затраты практически на все рутинные операции с документами (создание, поиск, согласование и т.д.). Кроме того, происходит ускорение документооборота и, как следствие, всех процессов в организации;
- *исключение несанкционированного доступа* - в отличие от традиционного «бумажного» документооборота, СЭД обеспечивает доступ к документам строго в соответствии с назначенными правами пользователей, все действия над документом (чтение, изменение, подписание) протоколируются;
- *прозрачность бизнес-процессов* - система обеспечивает возможность отслеживания этапов выполнения бизнес-процессов, что делает всю деятельность в организации абсолютно прозрачной для руководства и контролируемой;

- *повышение исполнительской дисциплины* - предоставляя полный контроль всех этапов работ для руководства, СЭД напрямую влияет на исполнительскую дисциплину сотрудников;
- *легкость внедрения инноваций и обучения* - благодаря системе оповещения, построенной на базе СЭД, можно быстро доводить новые правила работы до всех сотрудников. Сокращаются сроки обучения новых сотрудников. Легко меняются маршруты прохождения и шаблоны документов, после чего сотрудники автоматически начинают работать по-новому;
- *развитие корпоративной культуры* - процесс внедрения электронного документооборота налаживает и поддерживает корпоративную культуру. Возрастает ответственность каждого сотрудника за качественное выполнение выданного ему задания;
- *рост конкурентных преимуществ* - внедрение СЭД напрямую отражается на конкурентных преимуществах компании перед другими игроками рынка. Повышается скорость и качество обслуживания клиентов за счет ускорения движения информационных потоков и четкого контроля всех процессов.

Системы электронного документооборота функционируют на предприятиях и учреждениях, работающих в самых разных отраслях и сферах деятельности.

Базовые составляющие СЭД. Рассмотрим базовые составляющие современной системы электронного документооборота, необходимые для обеспечения поддержки работы предприятий с развитыми связями. К базовым составляющим СЭД относятся следующие подсистемы:

- идентификация и аутентификация пользователей;
- разграничение доступа к объектам;
- автоматизация управления потоками работ;
- управление электронными документами;
- регистрация событий в СЭД.

Подсистема идентификации и аутентификации пользователей. Идентификация и аутентификация обычно осуществляются путем набора системного имени и пароля (пара логин-пароль). Эти данные хранятся на сервере в специальной базе данных пользователей, причем в большинстве случаев предъявляется требование хранить их или только пароль в защищенном виде. В качестве механизма защиты может быть использовано шифрование или хэширование. В последнее время для подтверждения полномочий пользователя используют специальные носители информации (USB-ключи, смарт-карты).

Реализация рассматриваемой подсистемы может отличаться в разных системах электронного документооборота. В частности, эта подсистема может быть выделена в отдельный модуль или включена в исполняемый код клиентских приложений.

Подсистема разграничения доступа к объектам. В любой системе электронного документооборота обязательно должно быть предусмотрено разграничение прав пользователя. Разграничение прав пользователей внутри системы технически выполняется по-разному: это может быть полностью своя подсистема, созданная разработчиками СЭД, или подсистема безопасности СУБД, которую использует СЭД. Иногда их разработки комбинируют, используя свои разработки и подсистемы СУБД. Такая комбинация предпочтительнее, она позволяет закрыть возможные недостатки подсистем безопасности СУБД.

Подсистема автоматизации управления потоками работ. Подсистема автоматизации управления потоками работ (WorkFlow) реализует все функции, относящиеся к контролю исполнения: создание поручений исполнителям, задание сроков исполнения для поручений и всего документа, создание подпоручений, назначение контролеров поручений и документов, отслеживание сроков работ над поручениями и документами, рассылка уведомлений о назначении контролерами и исполнителями, а также уведомлений о приближении и истечении сроков работ.

Система управления потоками работ тесно интегрирована с почтовой системой, используемой электронным документооборотом. Это может быть своя собственная почтовая система или стандартная электронная почта.

Подсистема управления электронными документами. Эта система обеспечивает создание электронных документов, их перемещение между клиентом и сервером, перемещение между пользователями, поиск, просмотр, организацию процесса редактирования, а также удаление документов. Указанная функциональность может быть реализована в различных программных модулях, ее локализация в рамках одного модуля встречается достаточно редко. Для реализации перечисленных действий требуется совместная работа как клиента, так и сервера.

Подсистема регистрации событий в СЭД. Протоколирование действий пользователей в системах электронного документооборота является общепринятой функцией. Это необходимо как для обеспечения информационной безопасности, так и для выяснения истории документов. Возможны различные варианты реализации настроек протоколов и их просмотра. Следует отметить также применение в СЭД подсистем формирования отчетов, дизайнирования отчетных форм и регистрационных карточек, администрирования и хранения документов.

Распределенный электронный документооборот. После успешной автоматизации делопроизводства предприятия возникает задача автоматизации взаимодействия смежных организаций. Примером такого взаимодействия является обмен документами и распоряжениями между центральным офисом холдинга и

его филиалами, аналогичные задачи возникают и внутри крупной организации (общение подразделений между собой).

При рассмотрении схемы построения распределенного документооборота наиболее естественным вариантом является схема с единым центральным сервером. Этот сервер может выполнять различные функции - хранилища контактной информации о серверах предприятий, хранилища информации о пользователях, зарегистрированных на различных серверах, и хранилища документов, введенных в систему всеми участвующими в документообороте предприятиями.

Такая централизованная схема имеет очевидные достоинства, обусловленные простой процедурой установления связи между серверами и возможностью поиска чужих документов. Однако ее недостатком является нарушение работоспособности всего комплекса в случае выхода из строя центрального компьютера. Кроме того, в этом случае возникает проблема репликации данных между серверами, что само по себе непросто как технически, так и организационно.

Другой вариант архитектуры распределенной СЭД - схема с равноправными серверами предприятий. Этот вариант предполагает, что все участвующие в системе серверы абсолютно равноправны с точки зрения их программного обеспечения, а «выделенность» сервера центрального офиса проявляется в логике работы пользователей, в бизнес-логике, а не в технической реализации. К преимуществам такой схемы можно отнести жизнеспособность системы при сбоях отдельных серверных компьютеров, простоту настройки системы в целом, отсутствие репликации данных. Конечно, простота настройки, заключающаяся в отсутствии необходимости обслуживания центрального сервера, приводит к усложнению настройки каждого сервера системы. Это выражается в том, что для каждой пары взаимодействующих серверов потребуется задать некоторый набор настроек, позволяющий передавать данные между ними - адреса для связи (IP, e-mail), список пользователей, правила приема документов и ряд других.

В любой СЭД работа с документами регламентируется с помощью системы разграничения прав доступа к объектам. В данном случае предполагается, что права доступа будут задаваться сотрудникам внешних предприятий по той же схеме, что и для своих коллег. Принципиально возможна схема организации работы, направленная на ограничение выхода информации за пределы предприятия, что может быть реализовано несколькими способами, например введением рабочего места цензора или предоставлением права отправлять документы в посторонние организации ограниченному кругу сотрудников. Вариант действий выбирает заказчик системы исходя из степени закрытости сведений, хранимых и обрабатываемых СЭД.

Рассмотрим некоторые технические вопросы реализации обмена данными между серверами СЭД.

Для связи между серверными компьютерами могут быть применены несколько низкоуровневых протоколов. Наиболее предпочтительным для передачи данных в этом случае является использование стандартных интернет-протоколов HTTP (обычно используемый интернет-браузерами) и SMTP (протокол электронной почты). К преимуществам первого можно отнести распространенность и простоту, к недостаткам - отсутствие обработки ситуации отсутствия соединения и шифрования трафика, причем второй недостаток может быть устранен с помощью протокола шифрования SSL.

Что касается почтового протокола SMTP, главное его достоинство как раз в возможности корректной работы при разрыве соединения, обеспечиваемой развитой инфраструктурой серверов электронной почты. Недостаток - сравнительно невысокая скорость обмена, вызванная наличием этой самой инфраструктуры. Что касается безопасности передаваемых данных, она может быть обеспечена шифрованием пересылаемых писем и приложенных файлов любыми криптосредствами.

Для передачи данных может использоваться сравнительно высокоуровневый протокол SOAP (Simple Object Access Protocol - простой протокол для доступа к объектам), основной особенностью которого является возможность применения для низкоуровневой передачи данных как SMTP, так и HTTP с SSL. Выбор между этими протоколами может быть сделан при внедрении системы с учетом требований конкретного заказчика.

5.2. Особенности защиты электронного документооборота

Внедрение системы электронного документооборота обеспечивает компании большую гибкость в обработке и хранении информации и заставляет сотрудников компании работать быстрее и с большей отдачей. В то же время применение СЭД порождает новые риски и пренебрежение защитой обязательно приведет к новым угрозам безопасности. Внедряя СЭД, нельзя забывать о безопасности корпоративной информационной системы.

Базовым элементом любой СЭД является документ; внутри системы это может быть файл, а может быть запись в базе данных. Говоря о защищенном документообороте, часто подразумевают именно защиту документов, защиту той информации, которую они в себе несут. Однако на самом деле нужно заботиться о защите всей системы электронного документооборота, а не только о защите данных внутри нее. Это означает, что нужно защитить работоспособность СЭД, обеспечить быстрое восстановление после повреждений, сбоев и даже после уничтожения. Поэтому к защите системы электронного документооборота необходим комплексный подход, который подразумевает защиту на всех уровнях СЭД, начиная от защиты физических носителей информации, данных на них и заканчивая организационными мерами.

Таким образом, защита необходима, во-первых, аппаратным элементам системы. Это компьютеры, серверы, элементы компьютерной сети и сетевое оборудование. Во-вторых, защита необходима файлам системы. Это файлы программного обеспечения и базы данных. В случае их незащищенности появляется возможность воздействия злоумышленника на файлы СЭД. Например, файлы базы данных могут быть скопированы злоумышленником или повреждены в результате сбоя операционной системы или оборудования. В-третьих, необходимо защищать документы и информацию, находящиеся внутри системы.

Используя такой подход, можно построить систему, защищенную на всех уровнях, с рубежами обороны от угроз на каждом уровне. Стоимость такой защиты может сравняться со стоимостью самой СЭД, поэтому нужно искать разумный баланс между безопасностью и стоимостью.

5.2.1. Угрозы для СЭД

Угрозы для системы электронного документооборота могут быть классифицированы следующим образом.

Угроза целостности - повреждение и уничтожение информации, искажение информации как не намеренное в случае ошибок и сбоев, так и злоумышленное.

Угроза конфиденциальности - это любое нарушение конфиденциальности, в том числе кража, перехват информации, изменение маршрутов следования.

Угроза работоспособности системы - всевозможные угрозы, реализация которых приведет к нарушению или прекращению работы системы; сюда входят как умышленные атаки, так и ошибки пользователей, а также сбои в оборудовании и программном обеспечении.

Защиту от этих угроз должна реализовывать любая система электронного документооборота. Упорядочение документооборота позволяет выстроить более качественную систему защиты.

Можно выделить несколько основных групп источников угроз: легальные пользователи системы, административный ИТ-персонал, внешние злоумышленники. Согласно многочисленным исследованиям от 70 до 80% потерь от преступлений приходятся на атаки изнутри.

Пользователь системы является потенциальным злоумышленником, он может сознательно или несознательно нарушить конфиденциальность информации. Спектр возможных злоумышленных действий легальных пользователей достаточно широк - от скрепок в аппаратных частях системы до кражи информации с корыстной целью. При этом возможна реализация угроз в разных классах: угрозы конфиденциальности, угрозы целостности, угрозы работоспособности.

Особую группу составляет административный ИТ-персонал или персонал службы ИТ-безопасности. Эта группа, как правило, имеет неограниченные полномочия и доступ к хранилищам данных, поэтому к ней нужно относиться с особым вниманием. Они не только имеют большие полномочия, но и наиболее квалифицированы в вопросах безопасности и информационных возможностей. Состав внешних злоумышленников сугубо индивидуален. Это могут быть и конкуренты, и партнеры, и даже клиенты.

5.2.2. Средства защиты СЭД

Рассмотрим более подробно средства защиты, интегрированные в сами СЭД. Любая защищенная СЭД должна иметь средства защиты для выполнения следующих функций:

- обеспечение сохранности документов;
- обеспечение безопасного доступа;
- обеспечение конфиденциальности;
- обеспечение подлинности документов;
- протоколирование действий пользователей.

Обеспечение сохранности документов. СЭД должна обеспечить сохранность документов от потери и порчи и иметь возможность их быстрого восстановления. Согласно статистике потери важной информации в 45% случаев приходятся на физические причины (отказ аппаратуры, стихийные бедствия и подобное), 35% обусловлены ошибками пользователей и менее 20% - действием вредоносных программ и злоумышленников.

Представители половины компаний, переживших потерю данных, заявляют, что причиной инцидента стал саботаж или халатное отношение сотрудников к политике информационной безопасности компании, и только 20% респондентов сообщили, что интеллектуальная собственность их компаний защищена должным образом. Например, СЭД, использующие базы данных Microsoft SQL Server или Oracle, предпочитают пользоваться средствами резервного копирования от разработчика СУБД (в данном случае Microsoft или Oracle). Иные системы имеют собственные подсистемы резервного копирования, разработанные непосредственно производителем СЭД.

Обеспечение безопасного доступа. Безопасный доступ к данным внутри СЭД обеспечивается аутентификацией и разграничением прав доступа к объектам.

В СЭД могут использоваться различные методы *аутентификации*. Самый распространенный из них - применение многоразовых паролей. Шифрованные значения паролей обычно хранятся на сервере в специальной базе данных пользователей. Однако надежность данного метода сильно снижает человеческий фактор. Даже если пользователь использует правильно сгенерированный пароль, иногда его можно

обнаружить записанным на листке бумаги в столе или под клавиатурой. Часто полномочия пользователя подтверждаются специальным носителем информации. Существует множество решений для имущественной аутентификации пользователя: это USB-ключи, смарт-карты, магнитные карты, дискеты и CD. Здесь также не исключено влияние человеческого фактора, но злоумышленнику необходимо получить не только сам ключ, но и узнать PIN-код.

Надежным для проведения идентификации и последующей аутентификации является биометрический метод, при котором пользователь идентифицируется по своим биометрическим данным (это может быть отпечаток пальца, сканирование сетчатки глаза). Однако стоимость решения в этом случае выше, а современные биометрические технологии еще не настолько совершенны, чтобы избежать ложных срабатываний или отказов.

Важным параметром аутентификации является количество учитываемых факторов. Процесс аутентификации может быть однофакторным, двухфакторным и т.д. Возможно также комбинирование различных методов: парольного, имущественного и биометрического. Например, аутентификация может проходить при помощи пароля и отпечатка пальца (двухфакторный способ).

Разграничение прав доступа к объектам системы электронного документооборота может быть реализовано исходя из различных принципов:

- задание пользователей и групп, имеющих право чтения, редактирования или удаления всего документа, включая присоединенные файлы и реквизиты;
- мандатный доступ по группам, когда доступ к данным предоставляется в соответствии с фиксированными уровнями полномочий групп пользователей;
- разграничение доступа к различным частям документов, например к различным присоединенным файлам, группам реквизитов, полям регистрационных карточек, поручениям по документу.

Среди методов разграничения доступа можно выделить:

- задание доступа на уровне серверной базы данных;
- ограничение доступа на интерфейсном уровне, когда ряд действий не может быть выполнен через пользовательский интерфейс, но доступен в случае написания отдельной программы.

Обеспечение конфиденциальности. Обеспечение конфиденциальности информации осуществляется с помощью криптографических методов защиты данных. Их применение позволяет не нарушить конфиденциальность документа даже в случае его попадания в руки стороннего лица. Не стоит забывать, что любой криптографический алгоритм обладает таким свойством, как криптостойкость, т.е. и его защите есть предел. Нет шифров, которые нельзя было бы взломать. Это вопрос только времени и средств. Те алгоритмы, которые еще несколько лет назад считались надежными, сегодня уже успешно взламываются.

Поэтому для обеспечения конфиденциальности следует убедиться, что за время, потраченное на взлом зашифрованной информации, она либо безнадежно устареет, либо средства, потраченные на ее взлом, превзойдут стоимость самой информации. Кроме того, не следует забывать об организационных мерах защиты. Какой бы эффективной криптография ни была, ничто не помешает третьему лицу прочитать документ, например, стоя за плечом человека, который имеет к нему доступ, или расшифровать информацию, воспользовавшись ключом, который лежит в столе сотрудника.

Обеспечение подлинности документов. При организации электронного документооборота необходимо обеспечить юридическую значимость электронных документов в соответствии с российским законодательством. Эту задачу можно решить, используя систему электронной цифровой подписи и инфраструктуру управления открытыми ключами PKI.

Основной принцип работы ЭЦП основан на технологии шифрования с асимметричным ключом, при которой ключи для шифрования и расшифрования данных различны. Имеется «закрытый» ключ, который позволяет зашифровать информацию, и имеется «открытый» ключ, при помощи которого можно эту информацию расшифровать, но с его помощью невозможно «зашифровать» эту информацию. Таким образом, владелец цифровой подписи должен владеть «закрытым» ключом и не допускать его передачу другим лицам, а «открытый» ключ может распространяться публично для проверки подлинности цифровой подписи, полученной при помощи «закрытого» ключа. Подписать электронный документ с использованием ЭЦП может только обладатель «закрытого ключа», а проверить наличие ЭЦП - любой участник электронного документооборота, получивший «открытый ключ», соответствующий «закрытому ключу» отправителя. Успешная проверка ЭЦП показывает, что электронный документ подписан именно тем, от кого он исходит, и что он не был модифицирован после наложения ЭЦП.

Подтверждение принадлежности «открытых ключей» конкретным лицам осуществляет Удостоверяющий центр инфраструктуры управления открытыми ключами PKI - специальная организация, которой доверяют все участники информационного обмена. Обращение в Удостоверяющий центр позволяет каждому участнику убедиться, что имеющиеся у него копии «открытых ключей», принадлежащих другим участникам (для проверки их ЭЦП), действительно принадлежат этим участникам.

Большинство производителей СЭД имеют встроенные в свои системы, собственноручно разработанные или партнерские средства для использования ЭЦП, как, например, в системах Directum или «Евфрат-Документооборот». Такой тесной интеграции с ЭЦП немало способствовал и выход Федерального закона об ЭЦП (№ 1-ФЗ от 10.01.2002г.), согласно которому электронная цифровая подпись имеет юридическую силу наряду с собственноручной подписью.

Протоколирование действий пользователей. Важным моментом в защите электронного документооборота является протоколирование действий пользователей. Его правильная реализация в системе позволяет отследить все неправомерные действия и найти виновника, а при оперативном вмешательстве даже пресечь попытку неправомерных или наносящих вред действий.

Такая возможность обязательно должна присутствовать в самой СЭД. Кроме того, дополнительно можно воспользоваться решениями сторонних разработчиков и партнеров, чьи продукты интегрированы с СЭД. Прежде всего следует отметить СУБД и хранилища данных, любой подобный продукт крупных разработчиков, таких, как Microsoft или Oracle, наделен этими средствами. Также можно использовать возможности операционных систем по протоколированию действий пользователей.

Комплексный подход к защите электронного документооборота. При формировании защиты электронного документооборота необходимо объективно оценить возможные угрозы и риски СЭД и величину возможных потерь от реализованных угроз. Как уже отмечалось, защита СЭД не сводится только лишь к защите документов и разграничению доступа к ним. Необходимо обеспечить защиту аппаратных средств системы, персональных компьютеров, принтеров и прочих устройств, защиту сетевой среды, в которой функционирует система, защиту каналов передачи данных и сетевого оборудования.

На каждом уровне защиты важную роль играет комплекс организационных мер (инструктаж, подготовка персонала к работе с конфиденциальной информацией). Защита системы электронного документооборота должна быть комплексной.

О законодательном и нормативном регулировании. Вопросы обеспечения безопасности электронного документооборота решаются на основе законодательной и нормативной базы в области защиты информации. К законодательной базе в первую очередь относятся:

- Закон РФ «Об информации, информационных технологиях и защите информации»;
- Закон РФ «Об электронной цифровой подписи»;
- Государственная система сертификации продуктов защиты данных и лицензирования деятельности по предоставлению услуг в области защиты информации.

К нормативной базе относятся:

- стандарты криптографической защиты данных;
- требования и положения Гостехкомиссии РФ к средствам защиты информации от НСД.

Кроме указанных существует еще ряд стандартов информационной безопасности (см. гл. 12).

5.3. Защита баз данных

База данных представляет собой важнейший корпоративный ресурс, который должен быть надлежащим образом защищен с помощью соответствующих средств от любых умышленных или непредумышленных угроз. Понятие защиты применимо не только к данным, хранящимся в базе данных. Защита базы данных должна охватывать используемое оборудование, программное обеспечение, персонал и собственно данные.

Обсудим проблемы защиты базы данных с точки зрения таких потенциальных опасностей, как

- похищение и фальсификация данных;
- утрата конфиденциальности (нарушение тайны);
- нарушение неприкосновенности личных данных;
- нарушение целостности данных;
- потеря доступности данных.

Отмеченные опасности указывают основные направления, в которых нужно принимать меры, снижающие степень риска, т.е. потенциальную возможность потери или повреждения данных.

Похищение и фальсификация данных могут происходить не только в среде базы данных - вся организация так или иначе подвержена этому риску. Однако действия по похищению или фальсификации информации всегда совершаются людьми, поэтому основное внимание должно быть сосредоточено на сокращении общего количества удобных ситуаций для выполнения подобных действий.

Понятие конфиденциальности означает необходимость сохранения данных в тайне. Конфиденциальными считаются только те данные, которые являются важными для всей организации, тогда как понятие *неприкосновенности данных* касается требования защиты информации об отдельных сотрудниках. Следствием нарушения в системе защиты, вызвавшего потерю конфиденциальности данных, может быть утрата надежных позиций в конкурентной борьбе, тогда как следствием нарушения неприкосновенности личных данных могут стать судебные действия в отношении организации.

Нарушение целостности данных приводит к искажению или разрушению данных, что может иметь серьезные последствия для дальнейшей работы организации. В настоящее время множество организаций функционирует в непрерывном режиме, предоставляя свои услуги клиентам 24 часа в сутки и 7 дней в неделю.

Потеря доступности данных будет означать, что либо данные, либо система, либо и то и другое одновременно окажутся недоступными пользователям, а это может подвергнуть опасности финансовое положение организации.

Цель защиты базы данных - минимизировать потери, вызванные перечисленными и другими возможными событиями.

Принимаемые решения должны обеспечивать эффективное возмещение понесенных затрат и исключать излишнее ограничение предоставляемых пользователям возможностей.

5.3.1. Основные типы угроз

Угроза может быть вызвана ситуацией (или событием), способной принести ущерб организации, причиной которой может служить человек, происшествие или стечение обстоятельств. Любая угроза должна рассматриваться как потенциальная возможность нарушения системы защиты, которая в случае успешной реализации может оказать то или иное негативное влияние.

Приведем некоторые примеры возможных угроз для баз данных:

- похищение данных, программ и оборудования;
- несанкционированное изменение или копирование данных;
- просмотр и раскрытие засекреченных данных;
- создание «лазеек» в системе;
- внедрение компьютерных вирусов;
- использование прав доступа другого лица;
- ввод некорректных данных;
- пожары, наводнения, диверсии и др.

5.3.2. Методы и средства защиты СУБД

В отношении угроз, которые могут оказать отрицательное воздействие на работу базы данных, должны быть приняты контрмеры, начиная от физического контроля и заканчивая административно-организационными процедурами. Следует отметить, что общий уровень защищенности СУБД определяется возможностями используемой операционной системы, поскольку работа этих двух компонентов тесно связана между собой.

Для обеспечения информационной безопасности СУБД применяются следующие методы и средства защиты:

- авторизация пользователей;
- применение представлений;
- шифрование данных;
- поддержка целостности;
- резервное копирование и восстановление;
- применение RAID-массивов.

Авторизация пользователей. Под авторизацией понимают предоставление прав (или привилегий), позволяющих их владельцу иметь законный доступ к системе или к ее объектам. Термин «владелец» в приведенном выше определении может обозначать пользователя - человека или программу. Термин «объект» может обозначать таблицу данных, представление, приложение, процедуру или другой объект, который может быть создан в рамках системы. Средства авторизации пользователей могут быть встроены непосредственно в программное обеспечение и управлять не только предоставленными пользователям правами доступа к системе или объектам, но и набором операций, которые пользователи могут выполнять с каждым доступным ему объектом. По этой причине механизм авторизации часто называют средствами управления доступом.

За предоставление пользователям доступа к компьютерной системе обычно отвечает системный администратор, в обязанности которого входит создание учетных записей пользователей. Каждому пользователю присваивается уникальный идентификатор, который используется операционной системой для определения кто есть кто. С каждым идентификатором связывается определенный пароль, выбираемый пользователем и известный операционной системе. При регистрации пользователь должен предоставлять системе свой пароль для выполнения проверки (аутентификации) того, является ли он тем, за кого себя выдает. Подобная процедура позволяет организовать контролируемый доступ к компьютерной системе, но не обязательно предоставляет право доступа к СУБД или иной прикладной программе. Для получения пользователем права доступа к СУБД может использоваться отдельная такая процедура. Существует ряд других решений для аутентификации пользователя: это USB-ключи, смарт-карты, магнитные карты, цифровые сертификаты, средства биометрической аутентификации.

Ответственность за предоставление прав доступа к СУБД обычно несет администратор базы данных (АБД), в обязанности которого входит создание отдельных идентификаторов пользователей в среде самой СУБД. В некоторых СУБД ведется список идентификаторов пользователей и связанных с ними паролей, отличающийся от аналогичного списка, поддерживаемого операционной системой.

Привилегии. Как только пользователь получает право доступа к СУБД, ему могут автоматически предоставляться различные привилегии, связанные с его идентификатором. В частности, эти привилегии

могут включать разрешение на доступ к определенным базам данных, таблицам и представлениям, а также на создание этих объектов или же право вызывать на выполнение различные утилиты СУБД.

Привилегии предоставляются пользователям, чтобы они могли выполнять задачи, которые относятся к кругу их должностных обязанностей. Предоставление излишних или ненужных привилегий может привести к нарушению защиты, поэтому пользователь должен получать только такие привилегии, без которых он не имеет возможности выполнять свою работу.

Некоторые типы СУБД функционируют как *закрытые системы*, поэтому пользователям помимо разрешения на доступ к самой СУБД потребуется иметь отдельные разрешения и на доступ к конкретным ее объектам. Эти разрешения выдаются либо АБД, либо владельцами определенных объектов системы. В противоположность этому *открытые системы* по умолчанию *предоставляют* пользователям, прошедшим проверку их подлинности, полный доступ ко всем объектам базы данных. В этом случае привилегии устанавливаются посредством явной отмены тех или иных прав конкретных пользователей.

Права владения и привилегии. Как правило, владение некоторым объектом СУБД предоставляет его владельцу весь возможный набор привилегий в отношении этого объекта. Это правило применяется ко всем авторизованным пользователям, получающим права владения определенными объектами.

Любой вновь созданный объект автоматически передается во владение его создателю, который и получает весь возможный набор привилегий для данного объекта. Хотя при этом пользователь может быть владельцем некоторого представления, единственной привилегией, которая будет предоставлена ему в отношении этого объекта, может оказаться право выборки данных из тайного представления. Причина подобных ограничений состоит в том, что указанный пользователь имеет ограниченный набор прав в отношении базовых таблиц созданного им представления.

Принадлежащие владельцу привилегии могут быть переданы им другим авторизованным пользователям. Например, владелец нескольких таблиц базы данных может предоставить другим пользователям право выборки информации из этих таблиц, но не позволит им вносить в таблицы какие-либо изменения. В языке SQL предусмотрено, что если пользователь передает какие-либо привилегии, он может указать, приобретает ли получатель этих привилегий право передавать эти привилегии другим пользователям.

Если СУБД поддерживает несколько различных типов идентификаторов авторизации, с каждым из существующих типов могут быть связаны различные приоритеты. В частности, если СУБД поддерживает использование идентификаторов отдельных пользователей и групп, то, как правило, идентификатор пользователя будет иметь более высокий приоритет, чем идентификатор группы. В некоторых СУБД пользователю разрешается указывать, под каким идентификатором он намерен работать далее. Это целесообразно в тех случаях, когда один и тот же пользователь может являться членом сразу нескольких групп.

Применение представлений. *Представление* - динамический результат одной или нескольких реляционных операций с базовыми отношениями с целью создания некоторого иного отношения. Представление является *виртуальным отношением*, которое реально в базе данных не существует, но создается по требованию отдельного пользователя в момент поступления этого требования.

Механизм представлений служит мощным и гибким инструментом организации защиты данных, позволяющим скрывать от определенных пользователей некоторые части базы данных. В результате пользователи не будут иметь никаких сведений о существовании любых атрибутов или строк данных, которые не доступны через представления, находящиеся в их распоряжении.

Представление может быть определено на базе нескольких таблиц, после чего пользователю будут предоставлены необходимые привилегии доступа к этому представлению, но не к базовым таблицам. В данном случае использование представления устанавливает более жесткий механизм контроля доступа, чем обычное предоставление пользователю тех или иных прав доступа к базовым таблицам.

Шифрование данных. Традиционным способом обеспечения конфиденциальности данных является их шифрование. В процессе длительной эволюции серверов баз данных шифрование данных не применялось в течение многих лет. Шифрование данных в базах данных стало возможным только в последние годы, когда мощность процессоров достигла определенного уровня. В современных СУБД для шифрования данных в таблицах используется симметричное шифрование. Самым простым вариантом для пользователя является *«прозрачное шифрование данных»* (transparent data encryption). Эта технология базируется на управлении ключами системными средствами.

Ключевая информация, используемая для шифрования данных, хранится в специальном файле - «бумажнике» (wallet). Для доступа к бумажнику определен пароль «walletpsw». Для того чтобы открыть бумажник, необходимо предъявить файл и указать правильный пароль. Следует отметить, что в реальной системе хранить критически важную информацию в общеизвестном месте не самое лучшее решение.

Изменение таблицы, связанное с шифрованием столбца, требует наличия открытого бумажника. Для доступа к информации, хранящейся в зашифрованном столбце, также необходимо открыть бумажник. Бумажник открывается только один раз любым из пользователей, имеющих право на выполнение операции. Естественно, что после выполнения операций с закрытыми столбцами бумажник рекомендуется закрыть. Важно отметить, что после того как законный пользователь открыл бумажник, содержимое таблицы становится доступным всем пользователям, имеющим право доступа к данным таблицы. Отмеченный факт

существенно ограничивает область применения технологии прозрачного шифрования для систем с высокими требованиями к информационной безопасности.

В ряде случаев более предпочтительным оказывается выбор технологии *шифрования данных с явным заданием ключа пользователем*. Использование данной технологии предполагает наличие процедуры управления ключами. Администратор безопасности должен определить технологию генерации и распределения ключей, процедуры распределения и отзыва ключей (в случае их компрометации), процедуры управления резервными копиями ключей. При этом целесообразно использовать технику хранения пользователем ключевой информации на внешнем носителе. В качестве внешнего носителя часто используют устройство хранения данных на флэш-памяти.

Отсутствие отработанных способов решения перечисленных задач или небрежное их выполнение может привести к серьезным негативным последствиям. Потеря ключа может быть связана, например, с разрушением физического средства его хранения. Возможна утеря физического средства хранения информации. В любом случае происходит необратимая потеря данных. Современные средства криптографии обладают высокой стойкостью, и потеря ключа в большинстве случаев означает потерю данных. В процедурах шифрования могут использоваться криптографические алгоритмы блочного шифрования DES, 3DES, AES и алгоритм потокового шифрования RC4. Шифрование может также использоваться для защиты данных при их передаче по линиям связи.

Поддержка целостности. Средства поддержки целостности данных также вносят определенный вклад в общую защищенность базы данных, поскольку они должны предотвратить переход данных в несогласованное состояние, а значит, исключить угрозу получения неправильных результатов. Средства обеспечения целостности баз данных включают автоматическую поддержку системы правил, описывающих допустимость и достоверность хранимых и вводимых значений [10]. Реляционная модель включает некоторые характерные правила, вытекающие из существа модели: ограничения домена и ограничения таблицы.

Целостность домена предполагает, что допустимое множество значений каждого атрибута является формально определенным. Существуют формальные способы проверки того, что конкретное значение атрибута в базе данных является допустимым. Строка не будет вставлена в таблицу, пока каждое из значений ее столбцов не будет находиться в соответствующем домене (множестве допустимых значений).

Целостность таблицы означает, что каждая строка в таблице должна быть уникальной. Хотя не все СУБД промышленного уровня требуют выполнения такого ограничения, возможность уникальной идентификации каждой строки представляется необходимой для большинства реальных приложений. Ограничения целостности позволяют гарантировать, что требования к данным будут соблюдаться независимо от способа их загрузки или изменения.

Резервное копирование и восстановление. *Резервное копирование* - периодически выполняемая процедура получения копии базы данных и ее файла журнала (а также, возможно, программ) на носителе, хранящемся отдельно от системы. Любая современная СУБД должна предоставлять средства резервного копирования, позволяющие восстанавливать базу данных в случае ее разрушения. Кроме того, рекомендуется создавать резервные копии базы данных и ее файла журнала с некоторой установленной периодичностью, а также организовывать хранение созданных копий в местах, обеспеченных необходимой защитой. В случае аварийного отказа, в результате которого база данных становится непригодной для дальнейшей эксплуатации, резервная копия и зафиксированная в файле журнала оперативная информация используются для восстановления базы данных до последнего согласованного состояния.

Ведение журнала представляет собой процедуру создания и обслуживания файла журнала, содержащего сведения обо всех изменениях, внесенных в базу данных с момента создания последней резервной копии, и предназначенного для обеспечения эффективного восстановления системы в случае ее отказа. СУБД должна предоставлять средства ведения системного журнала, в котором будут фиксироваться сведения обо всех изменениях состояния базы данных и о ходе выполнения текущих транзакций, что необходимо для эффективного восстановления базы данных в случае отказа.

Преимущества использования подобного журнала заключаются в том, что в случае нарушения работы или отказа СУБД базу данных можно будет восстановить до последнего известного согласованного состояния, воспользовавшись последней созданной резервной копией базы данных и оперативной информацией, содержащейся в файле журнала. Если в отказавшей системе функция ведения системного журнала не использовалась, базу данных можно будет восстановить только до того состояния, которое было зафиксировано в последней созданной резервной копии. Все изменения, внесенные в базу данных после создания последней резервной копии, будут потеряны.

Применение RAID-массивов. Аппаратное обеспечение, на котором эксплуатируется СУБД, должно быть отказоустойчивым. Это означает, что СУБД должна продолжать работать даже при отказе аппаратных компонентов. Для этого необходимо иметь избыточные компоненты, которые могут быть объединены в систему, сохраняющую свою работоспособность при отказе одного или нескольких компонентов. К числу основных аппаратных компонентов, которые должны быть отказоустойчивыми, относятся дисковые накопители, дисковые контроллеры, процессоры, источники питания и вентиляторы охлаждения. Дисковые накопители являются наиболее уязвимыми среди всех аппаратных компонентов и характеризуются самыми низкими показателями непрерывной работы между отказами.

Одним из решений этой проблемы является применение технологии RAID. Первоначально эта аббревиатура расшифровывалась как Redundant Array of Inexpensive Disks (массив недорогих дисковых накопителей с избыточностью), но в дальнейшем букву «I» в этой аббревиатуре стали рассматривать как сокращение от «independent» (независимый).

RAID-массив представляет собой массив дисковых накопителей большого объема, состоящий из нескольких независимых дисков, совместное функционирование которых организовано таким образом, что при этом повышается надежность и увеличивается производительность [4].

Производительность увеличивается благодаря полосовому распределению данных. Данные на дисках распределяются по сегментам, представляющим собой разделы дисков равного размера (этот размер называется *единицей полосового распределения)*, которые распределяются по нескольким дискам и обеспечивают прозрачный доступ. В результате такой массив становится аналогичным одному крупному быстродействующему диску, но фактически данные в нем распределены по нескольким дискам меньшего объема. Полосовое распределение обеспечивает повышение производительности ввода-вывода, поскольку позволяет одновременно выполнять несколько операций ввода-вывода (на разных дисках). Наряду с этим полосовое распределение данных позволяет равномерно распределять нагрузку между дисками.

Повышенная надежность RAID-массива обеспечивается благодаря дублированию данных (такие дубликаты называются *зеркальными копиями)* и хранению на дисках избыточной информации, сформированной с использованием схем контроля четности или схем исправления ошибок, таких, как корректирующий код Рида-Соломона (Reed-Solomon) [11].

В схеме контроля четности каждый байт должен иметь связанный с ним бит четности, который принимает значение 0 или 1 в зависимости от того, является ли четным или нечетным количество битов 1 в байте, которому соответствует этот бит контроля четности. Если в контролируемом байте некоторые биты будут искажены, значение бита четности не совпадет со значением, соответствующим новому составу битов 1 в этом байте. Аналогичным образом при искажении хранимого бита контроля четности он не будет соответствовать данным в байте, что позволит обнаружить ошибку. С другой стороны, схемы корректировки ошибок предусматривают хранение двух или больше дополнительных битов и позволяют восстанавливать первоначальные данные, если один из битов будет искажен. Схемы контроля четности и корректировки ошибок могут применяться при полосовом распределении данных по дискам.

В RAID-массивах используются различные сочетания описанных выше методов повышения производительности и надежности, получившие название уровней RAID. Эти уровни перечислены ниже.

- ***RAID 0*** (неизбыточный массив). На этом уровне не применяется дублирование данных и поэтому обеспечивается наивысшая производительность записи, поскольку не приходится копировать по дискам обновляемые данные. Полосовое распределение данных осуществляется на уровне дисковых блоков.
- ***RAID 1*** (массив с зеркальным отображением). На этом уровне ведутся две идентичные (зеркальные) копии данных на разных дисках. Для обеспечения сохранности данных на случай отказа диска запись на разные диски в некоторых вариантах реализации такого массива не выполняется одновременно. Этот вариант организации хранения данных во внешней памяти является наиболее дорогостоящим.
- ***RAID 0+1*** (неизбыточный массив с зеркальным отображением). На этом уровне применяется сочетание методов полосового распределения и зеркального отображения данных.
- ***RAID 2*** (массив с применением кодов корректировки ошибок, хранящихся во внешней памяти). На этом уровне единицей полосового распределения является один бит и для реализации схемы избыточности применяются корректирующие коды Хэмминга.
- ***RAID 3*** (массив, обеспечивающий контроль четности с чередованием битов). На этом уровне предусматривается хранение избыточных данных (представляющих собой информацию контроля четности) на отдельном диске массива. Эта информация может применяться для восстановления данных, хранящихся на других дисках, в случае отказа этих дисков. На этом уровне используется меньший дополнительный объем пространства внешней памяти по сравнению с уровнем RAID 1, но доступ к диску с информацией контроля четности может стать узким местом, ограничивающим производительность.
- ***RAID 4*** (массив, обеспечивающий контроль четности с чередованием блоков). На этом уровне единицей полосового распределения является блок диска; блоки с информацией контроля четности хранятся на ином диске, чем соответствующие блоки данных с нескольких других дисков. При отказе одного из дисков с данными блок контроля четности может применяться в сочетании с соответствующими блоками с других дисков для восстановления данных, которые хранились на отказавшем диске.
- ***RAID 5*** (массив, обеспечивающий контроль четности с чередованием блоков и распределением информации контроля четности). На этом уровне информация контроля четности применяется в качестве избыточной и обеспечивающей восстановление первоначальных данных по такому же принципу, как в массиве RAID 3, но данные контроля четности распределяются с помощью метода полосового распределения по всем дискам таким же образом, как происходит распределение исходных данных. Это позволяет устранить узкое место, возникающее, если вся информация контроля четности хранится на одном диске.
- ***RAID 6*** (массив с избыточностью P+Q). Этот уровень аналогичен уровню RAID 5, но предусматривает хранение дополнительных избыточных данных для защиты от отказа сразу нескольких дисков. При этом вместо информации контроля четности используются коды исправления ошибок.

Корпорация Oracle рекомендует использовать уровень RAID 1 для файлов журнала восстановления. А для файлов базы данных рекомендуется применение уровня RAID 5, если он обеспечивает приемлемые задержки при записи, а в ином случае рекомендуется уровень RAID 1 или RAID 0+1.

5.3.3. Средства защиты СУБД Microsoft Access

СУБД Microsoft Access 2000 предоставляет следующие два метода защиты базы данных:

- установка пароля, который применяется при открытии базы данных (это средство в терминологии Microsoft Access называется *защитой системы);*
- применение средств защиты на уровне пользователя, которые могут применяться для определения тех частей базы данных, в которых пользователь может выполнять операции чтения или обновления (это средство в терминологии Microsoft Access называется *защитой данных).*

Рассмотрим, как эти механизмы защиты реализованы в СУБД Microsoft Access [4].

Установка пароля. Самым простым методом защиты является установка пароля, применяемого для открытия базы данных. После установки пароля (в меню Tools Security) при любой попытке открыть базу данных на экране появляется диалоговое окно с приглашением ввести пароль. Разрешение открыть базу данных получают только те пользователи, которые вводят правильный пароль.

Этот метод является надежным, поскольку СУБД Microsoft Access шифрует пароль таким образом, чтобы его нельзя было определить непосредственно считывая файл базы данных, но после открытия базы данных все объекты, содержащиеся в ней, становятся доступными для пользователя.

Защита на уровне пользователя. Средства защиты на уровне пользователя в СУБД Microsoft Access аналогичны средствам, которые применяются в большинстве сетевых систем. При запуске программы Microsoft Access пользователи должны указать свой идентификатор и ввести пароль.

В файле с информацией о рабочих группах программы Microsoft Access пользователи обозначаются как члены некоторой группы. В СУБД Access предусмотрены по умолчанию две группы: администраторы (группа Admins) и пользователи (группа Users), но могут быть определены и дополнительные группы. Группам и пользователям предоставляются права доступа, которые позволяют регламентировать перечень допустимых для них операций с каждым объектом базы данных. Для этого применяется диалоговое окно Разрешения (User and Group Permissions).

В табл.5.1 приведен перечень прав доступа, которые могут быть установлены в СУБД Microsoft Access.

Таблица 5.1

Права доступа в СУБД Microsoft Access

Права доступа	Описание допустимых операций
Open/Run	Открывать базу данных, форму, отчет или вызывать макрокоманду на выполнение
Open Exclusive	Открывать базу данных с исключительными правами доступа
Read Design	Просматривать объекты в представлении Design
Modify Design	Просматривать, модифицировать и удалять объекты базы данных
Administer	Применительно к базам данных: устанавливать пароль базы данных, копировать базы данных и модифицировать сценарии запуска Применительно к объектам базы данных: полный доступ, в том числе возможность назначать права доступа
Read Data	Просматривать данные
Update Data	Просматривать и модифицировать данные (но не вставлять и удалять)
Insert Data	Просматривать и вставлять данные (но не модифицировать и удалять)
Delete Data	Просматривать и удалять данные (но не вставлять и модифицировать)

5.3.4. Средства защиты СУБД Oracle

В предыдущем разделе описаны два типа средств защиты в СУБД Microsoft Access: защита системы и защита данных. В данном разделе показано, как эти два типа средств защиты реализованы в СУБД Oracle.

Как и в СУБД Access, одна из форм защиты системы, применяемая в СУБД Oracle, предусматривает реализацию стандартного механизма проверки идентификатора и пароля пользователя, в соответствии с которым пользователь должен ввести действительный идентификатор и пароль и только после этого получить доступ к базе данных.

При каждой попытке пользователя подключиться к базе данных открывается диалоговое окно Connect или Log On с приглашением ввести идентификатор и пароль пользователя для доступа к указанной базе данных.

Привилегии. Привилегия представляет собой право выполнять операторы SQL определенного типа или обращаться к объектам другого пользователя. Ниже приведены примеры некоторых привилегий Oracle, которые позволяют выполнять определенные действия:

- подключение к базе данных (открытие сеанса);
- создание таблицы;
- выборка строк из таблицы другого пользователя.

В СУБД Oracle предусмотрены две категории привилегий:

- системные привилегии;
- привилегии на объекты.

Системная привилегия представляет собой право выполнять определенные действия или проводить операции с любыми объектами схемы определенного типа. Например, к системным относятся привилегии на создание табличных пространств и учетных записей пользователей базы данных.

В СУБД Oracle предусмотрено свыше 80 системных привилегий. Системные привилегии можно предоставлять пользователям и ролям (которые рассматриваются ниже) или отзывать эти привилегии с использованием любого из следующих средств:

- диалоговые окна Grant System Privileges/Roles и Revoke System Privileges/Roles программы Oracle Security Manager;
- операторы GRANT и REVOKE языка SQL.

Предоставлять или отзывать системные привилегии могут только пользователи, которым предоставлена специальная системная привилегия с помощью конструкции ADMIN OPTION, или пользователи с системной привилегией GRANT ANY PRIVILEGE.

Привилегией на объект является привилегия или право выполнять определенное действие с конкретной таблицей, представлением, последовательностью, процедурой, функцией или пакетом.

Для работы с объектами разных типов предоставляются различные привилегии на объекты. Например, одной из привилегий на объект является право удалять строки из таблицы Staff.

С некоторыми объектами схемы (такими, как кластеры, индексы и триггеры) не связаны привилегии на объекты; применение этих объектов регламентируется с помощью системных привилегий. Например, чтобы внести изменения в кластер, пользователь должен быть владельцем этого кластера или иметь системную привилегию ALTER ANY CLUSTER.

Пользователь автоматически приобретает все привилегии на объекты, содержащиеся в его схеме. Кроме того, пользователь может предоставить любому другому пользователю или роли привилегии на любые принадлежащие ему объекты схемы. Если в операторе SQL, применяемом для предоставления такой привилегии, включена опция WITH GRANT OPTION (оператора GRANT), лицо, получившее привилегию на объект, может предоставить ее другому пользователю; в противном случае он может использовать полученную привилегию, но не имеет право предоставлять ее другим пользователям. В табл.5.2 показаны привилегии на такие объекты, как таблицы и представления.

Таблица 5.2

Допустимые действия с таблицами и представлениями

Привилегия на объект	Таблица	Представление
ALTER	Модифицировать определение таблицы с применением оператора ALTER TABLE	Какие-либо действия не предусмотрены
DELETE	Удалять строки из таблицы с применением оператора DELETE. *Примечание*. Наряду с привилегией DELETE должна быть предоставлена привилегия SELECT	Удалять строки из представления с применением оператора DELETE
INDEX	Создавать индекс в таблице с применением оператора CREATE INDEX	Какие-либо действия не предусмотрены
INSERT	Вводить новые строки в таблицу с применением	Вводить новые строки в представление с

	оператора INSERT	применением оператора INSERT
REFERENCES	Создавать ограничение, которое ссылается на таблицу. Эта привилегия не может быть предо-ставлена роли	Какие-либо действия не предусмотрены
SELECT	Запрашивать данные в таблице с применением оператора SELECT	Запрашивать данные в представлении с применением оператора SELECT
UPDATE	Модифицировать данные в таблице с применением оператора UPDATE. *Примечание*. Наряду с привилегией UPDATE должна быть предоставлена привилегия SELECT	Модифицировать данные в представлении с применением оператора UPDATE

Роли. Пользователь может получить привилегию двумя способами:

- привилегии могут предоставляться пользователям явным образом, например пользователю Beech может быть явно предоставлена привилегия вставлять строки в таблицу PropertyForRent:

GRANT INSERT ON PropertyForRent TO Beech;

- привилегии могут также предоставляться некоторой *роли* (так называется именованная группа привилегий), а затем эта роль может предоставляться одному или нескольким пользователям. Например, привилегии на выборку, вставку и обновление строк в таблице PropertyForRent могут быть предоставлены роли Assistant, а эта роль, в свою очередь, может быть предоставлена пользователю Beech. Любой пользователь может иметь доступ к нескольким ролям, а нескольким пользователям могут быть назначены одинаковые роли. Поскольку роли позволяют проще и лучше управлять привилегиями, то привилегии, как правило, должны предоставляться ролям, а не отдельным пользователям.

5.3.5. Защищенный доступ к базам данных

В предыдущих разделах было показано, что СУБД от ведущих мировых производителей имеют встроенные механизмы защиты. Они позволяют:

- авторизовать пользователей при доступе к БД;
- разграничивать права пользователей на управление данными (например, одни пользователи могут только просматривать БД, а другие - делать в них добавления и изменения);
- разграничивать права пользователей на администрирование СУБД (операции по удалению старых или добавлению новых пользователей БД);
- разграничивать доступ пользователей к информации, хранящейся в БД.

Эти механизмы защиты позволяют обеспечить минимальный уровень безопасности.

Чтобы быть уверенным в безопасности своих компьютерных систем и обрабатываемых в них данных, использование перечисленных механизмов защиты недостаточно по следующим причинам.

- Пользователи базы данных, в том числе и ее администратор, могут назначить себе «слабые» пароли, которые легко подобрать. Кроме того, в некоторых СУБД аутентификационные данные администратора заложены на уровне программного кода и не могут быть изменены, хотя именно по этой причине они общеизвестны.
- Администраторы БД, порой, несвоевременно удаляют старые учетные записи, например, при увольнении сотрудников, и неиспользуемые пароли остаются действительными еще в течение долгого времени.
- Любая СУБД - это всего лишь программа, которую писали люди. Людям свойственно ошибаться. Ошибки в программном обеспечении могут при определенных условиях заставить программу функционировать неправильно. Такие ошибки называют уязвимостями. Именно ими и пользуются хакеры для проведения своих атак.
- Хакерские атаки не всегда могут быть направлены непосредственно на СУБД. Любая база данных функционирует на платформе определенной операционной системы, которая тоже может иметь уязвимые места. Если злоумышленник сможет получить контроль над самим сервером, то все встроенные в СУБД механизмы безопасности будут практически бесполезны.
- Целью злоумышленника не всегда является получение доступа к информации. Порой больше убытков может принести не разглашение информации, а недоступность для клиентов самого сервиса БД (например, простой системы продажи авиабилетов).

- Никогда нельзя быть уверенным в том, что выданным администратором паролем будет пользоваться один человек и что этот пароль не станет достоянием других людей.
- Информация, которая хранится и обрабатывается в базах данных, может быть конфиденциальна. Поэтому следует позаботиться о защите ее от перехвата в каналах связи.

Для обеспечения надежной защиты базы данных необходимо предпринять следующие меры (рис.5.1).

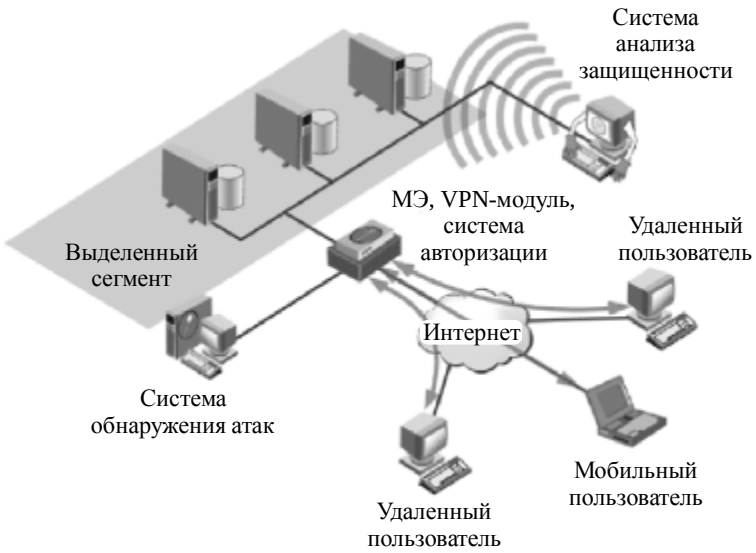

Рис.5.1. Схема защищенного доступа к базам данных

1. Поместить серверы, на которых размещается БД, в отдельный сегмент сети и защитить вход в него межсетевым экраном. На межсетевом экране нужно задать правила, которые закроют пользователям сервиса баз данных доступ ко всему, кроме этих баз. Это существенно снизит риск того, что система будет взломана.
2. Чтобы защититься от уязвимостей, которыми могут воспользоваться легальные пользователи БД, необходимо установить систему обнаружения атак. Она позволит обнаруживать возможную несанкционированную сетевую активность в пределах разрешенных протоколов. «Прослушивая» сетевой трафик и сопоставляя его с базой сигнатур атак, сетевой сенсор обнаруживает различные нарушения политики безопасности. Использование системы обнаружения атак, разработанной с учетом специфики СУБД, позволяет дополнительно повысить уровень защищенности данных.
3. Контролировать деятельность администратора на предмет правильного управления настройками СУБД позволит система анализа защищенности. Она вовремя обнаружит неправильно назначенные права доступа к таблицам и процедурам, выявит «слабые» пароли, обнаружит неиспользуемые учетные записи и т.п. Кроме того, она найдет в СУБД известные ей уязвимости и выдаст рекомендации по их устранению.
4. Защитить информацию от перехвата, а учетные записи - от возможного тиражирования помогут средства VPN. Благодаря использованию цифровых сертификатов можно выдавать пользователям не пароли для доступа, а персональные сертификаты на различных носителях, которые не подлежат копированию [22]. Это обеспечивает:
   - строгую криптографическую аутентификацию удаленных пользователей;
   - защиту данных, передаваемых в пределах рабочего сеанса;
   - невозможность осуществить «двойной» вход в систему с одним комплектом учетных данных.

5.4. Защита корпоративного почтового документооборота

Эффективная деятельность любого современного предприятия немыслима без наличия электронного документооборота. Работа с документами в электронной форме позволяет быстро и удобно хранить, обрабатывать и передавать их в рамках корпоративной информационной системы.

Перечисленные функции, как правило, выполняет почтовая система, являющаяся неотъемлемой частью всякого электронного документооборота [15]. Она включает в себя такие базовые элементы, как почтовые клиенты и почтовые серверы. Пример обобщенной архитектуры почтовой системы приведен на рис.5.2.

Почтовые клиенты представляют собой ПО, устанавливаемое на рабочих станциях пользователей ИС. Они с его помощью формируют, отправляют и получают электронные документы. Наиболее распространенными примерами почтовых клиентских программ являются Outlook компании Microsoft, а также программа The Bat! компании Rit Labs.

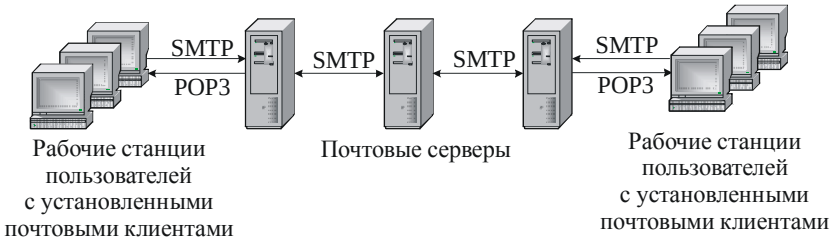

Рис.5.2. Обобщенная архитектура электронной почтовой системы

В свою очередь, почтовый сервер - это тоже ПО, оно устанавливается на выделенном серверном ресурсе. Посредством почтового клиента пользователь формирует документ и через механизм SMTP (Simple Mail Transfer Protocol) передает его на почтовый сервер для отправки адресату. Последний, используя свой почтовый клиент, подключается к почтовому серверу и загружает документ на ПК. Получение электронной почты осуществляется по протоколу POP3 (Post Office Protocol, версия 3). Для взаимодействия же самих почтовых серверов между собой применяется протокол SMTP. Почтовыми серверами являются продукт Exchange компании Microsoft и свободно распространяемое ПО sendmail.

Почтовая система, используемая в качестве основы электронного документооборота, обладает рядом преимуществ, основными из которых являются популярность данного сервиса среди пользователей компьютерных систем, быстрота доставки сообщений (электронная почта из России в США доставляется в среднем за 2 мин), а также низкая стоимость использования по сравнению с традиционной телефонной и факсимильной связью.

Следует, однако, иметь в виду, что любая почтовая система потенциально подвержена ряду угроз, которые способны привести к нарушению конфиденциальности, целостности или доступности информации. При этом угрозы безопасности системы могут исходить как со стороны внутренних пользователей, так и извне, например из сети Интернет.

Угрозы информационной безопасности воплощаются в реальных атаках злоумышленников. Объектами этих атак могут быть почтовые серверы, рабочие станции пользователей, а также информация, передаваемая между ними. Так, атакующий может поставить себе цель получить доступ к содержимому передаваемых почтовых сообщений и изменять его. Другой пример информационных атак - вторжение в ИС путем внедрения вирусов через почтовую систему.

Рассмотрим существующие методы и средства, позволяющие защитить почтовую систему от возможных угроз и, насколько это возможно, проиллюстрируем их функциональность.

Защита каналов сетевого взаимодействия почтовых клиентов и серверов. Известно, что в почтовых протоколах SMTP и POP3 нет встроенных механизмов защиты передаваемых данных. Поэтому у злоумышленника появляется неплохая возможность реализовать атаку, направленную на нарушение конфиденциальности и/или целостности пакетов данных, передаваемых посредством этих протоколов.

Защититься от атак подобного типа можно с помощью технологии VPN, позволяющей организовать между хостами ИС зашифрованные каналы связи. При этом управление защищенными сетевыми соединениями осуществляется с помощью специализированных криптопротоколов. Последние реализуются на различных уровнях модели взаимодействия открытых систем [1].

Виртуальные частные сети могут быть развернуты на базе сетевых ОС со встроенной VPN-функциональностью, активного сетевого оборудования, ПО которого поддерживает функции VPN, а также специализированного программно-аппаратного обеспечения, предназначенного для криптографической защиты информации.

Если средства защиты этого типа выполнены в виде автономных программно-аппаратных блоков, то они устанавливаются в каналы связи, в противном случае - на серверы и рабочие станции пользователей.

Обеспечение конфиденциальности и целостности электронных документов. Информационные атаки нередко предпринимаются для умышленного искажения передаваемых по сети электронных документов пользователей. Для защиты от таких атак могут быть применены средства, базирующиеся на технологии PKI (Public Key Infrastructure). Этой технологией предусмотрено использование асимметричных криптоалгоритмов на уровне самих электронных документов, а не пакетов данных.

Напомним, что асимметричная схема требует наличия двух разных криптографических ключей - открытого и закрытого. Такая схема обладает следующими особенностями:

- ключи могут существовать только в парах «открытый ключ - закрытый ключ». При этом одному открытому ключу соответствует только один закрытый ключ;
- значение закрытого ключа невозможно вычислить, имея доступ только к открытому ключу;
- открытый ключ свободно распространяется по общедоступным каналам связи, в то время как закрытый хранится в секрете.

Для безопасного обмена открытыми ключами между пользователями ИС служат цифровые сертификаты. Сертификат представляет собой структуру данных, содержащую открытый ключ владельца сертификата; он подписывается выдающей его службой. В качестве последней выступает так называемый

удостоверяющий центр. Таким образом, выдавая сертификат, удостоверяющий центр гарантирует соответствие открытого ключа субъекта идентифицирующей его информации.

Технология PKI обеспечивает целостность передаваемых в ИС документов посредством механизма электронной цифровой подписи. ЭЦП - это не что иное, как реквизит документа, позволяющий устанавливать отсутствие искажения содержащейся в документе информации, а также однозначно определять обладателя подписи. Формат электронного документа с ЭЦП должен соответствовать международным стандартам PKCS7 и S/MIME.

Криптографические методы, использующиеся в технологии PKI, также могут быть применены и для обеспечения конфиденциальности передаваемых через корпоративную почтовую систему электронных документов.

В этом случае защита электронных документов осуществляется посредством их шифрования открытыми ключами, содержащимися в сертификатах получателей этих документов. При этом зашифрованный документ должен соответствовать международному стандарту PKCS7. Для расшифровки документов их получатели используют свои закрытые ключи. Процедура работы с защищенным почтовым сообщением показана на рис.5.3.

Рис.5.3. Схема работы с защищенным почтовым сообщением

Для обеспечения криптографической защиты почтовых сообщений на рабочие станции пользователей нужно устанавливать дополнительные программные средства, реализующие технологию PKI. Эти средства выполняют следующие функции:

- шифрование/расшифрование почтовых сообщений с добавлением/проверкой ЭЦП;
- блокирование незащищенных криптографическими методами входящих и исходящих почтовых сообщений;
- ведение архива входящих и исходящих сообщений;
- ведение журнала аудита, в котором регистрируются все криптографические операции, выполненные над входящими и исходящими почтовыми сообщениями.

Обеспечение работоспособности почтовых серверов. Почтовые серверы ИС предприятия тоже могут стать объектами сетевых атак, направленных на нарушение их функционирования. Успешность атак этого типа возможна из-за уязвимостей, которые присутствуют в ПО почтовых серверов. Причинами возникновения таких уязвимостей являются плохое программирование, некорректная конфигурация почтовых сервисов и пр.

Чтобы защитить почтовые серверы от подобных атак, необходимо использовать средства, способные выполнять функции выявления и устранения уязвимостей, а также обнаружения и блокирования сетевых атак. Для выявления уязвимостей используют специализированные системы анализа защищенности - они сканируют серверы ИС предприятия. В случае обнаружения уязвимости такая система выдает рекомендации по ее устранению.

Выявить и своевременно блокировать сетевые атаки позволяют средства обнаружения вторжений и межсетевые экраны (МЭ). Последние обеспечивают фильтрацию запросов на уровне межсетевого взаимодействия и транспортном уровне стека TCP/IP и блокируют те из них, которые представляют потенциальную угрозу для почтовых серверов. Почтовый сервер подключается к МЭ таким образом, чтобы все запросы, поступающие к нему, проходили через экран.

В дополнение к МЭ для выявления и блокирования сетевых атак на прикладном уровне используются сетевые и серверные датчики обнаружения вторжений. Сетевые датчики устанавливаются перед и сзади МЭ и выполняют функции пассивного анализа и выявления атак на почтовый сервер. При этом датчик, установленный перед МЭ, вдобавок позволяет обнаруживать и атаки на сам экран. Для того чтобы не только обнаруживать, но и блокировать сетевые атаки, дополнительно на почтовый сервер необходимо установить датчик обнаружения вторжений уровня хоста, выполняющий функцию блокирования запросов, представляющих опасность для сервера.

Обеспечение антивирусной защиты почтовой системы. Почтовые системы предприятий могут быть использованы злоумышленниками для распространения вредоносных программ, например, таких, как информационные вирусы. Типичная вирусная атака на ИС реализуется так: злоумышленник помещает в

электронное письмо зараженный вирусом файл и рассылает его пользователям ИС; получение и открытие такого письма на рабочей станции автоматически вызывает запуск инфицированного исполняемого файла и система заражается информационным вирусом.

Один из способов антивирусной защиты корпоративной почтовой системы заключается в формировании в рамках ИС криптографически защищенной среды, в которой могут передаваться только зашифрованные и подписанные посредством ЭЦП сообщения. В этом случае любое не защищенное криптографическим методом сообщение рассматривается системой как потенциально опасное и подлежащее блокированию. Реализация такого способа требует установки на все рабочие станции пользователей ИС специализированного ПО. Для усиления защиты рекомендуется установить на рабочие станции антивирусное ПО.

Защита от утечки конфиденциальной информации. Злоумышленники могут использовать почтовую систему ИС предприятия и в качестве канала утечки конфиденциальной информации. В этом случае нарушитель, имея возможность сформировать почтовое сообщение, помещает в него конфиденциальные данные и отправляет за пределы ИС. При этом для отправки сообщений он может воспользоваться не только корпоративным, но и внешним почтовым сервером.

Эффективная защита от атак этого типа обеспечивается с помощью системы активного мониторинга (CAM) рабочих станций, позволяющей выявлять несанкционированные действия пользователей ИС. Размещаемые на рабочих станциях агенты CAM способны выявлять и блокировать нарушения установленной политики безопасности. В частности, для обеспечения защиты от утечки конфиденциальной информации администратор CAM может ограничить перечень адресатов, которым пользователи ИС отправляют сообщения, а также явно указать IP-адреса SMTP- и POP3-серверов - через них (и только через них!) пользователи имеют право работать с почтовой системой ИС.

Исходя из всего вышесказанного можно сделать очевидный вывод, что для организации эффективной защиты почтовой системы, входящей в состав ИС предприятия, необходимо создание комплексной системы безопасности, базирующейся на рассмотренных средствах. Описание такой системы приводится ниже.

Комплексный подход к защите корпоративной почтовой системы. Рассмотрим пример построения защищенной корпоративной почтовой системы, включающей в себя как почтовые серверы, так и локальных и удаленных пользователей. Локальные пользователи работают с почтовой системой, находясь внутри корпоративной ИС, а удаленные - вне ИС через сеть Интернет. Взаимодействие между пользователями и серверами осуществляется по протоколам SMTP и POP3. На рис.5.4 приведена архитектура защищенной системы электронной почты.

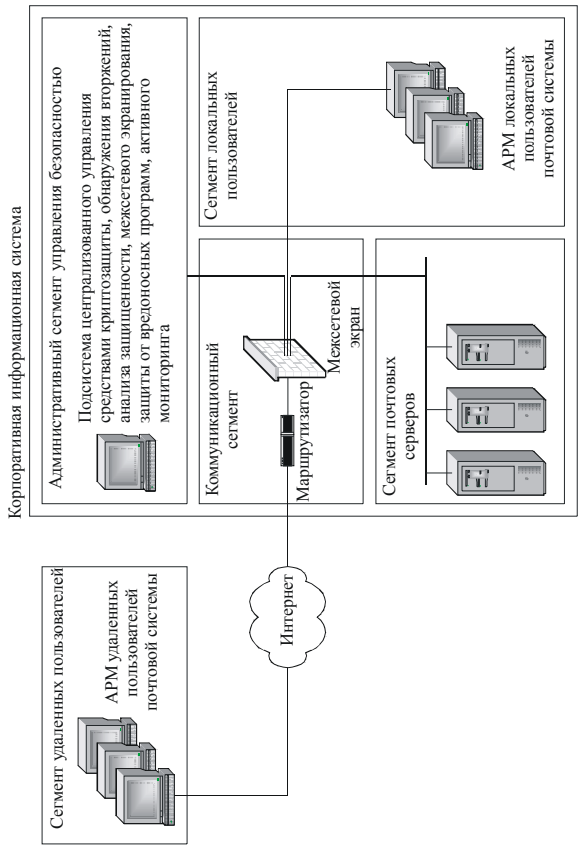

Рис.5.4. Архитектура защищенной системы электронной почты

Система обеспечения информационной безопасности электронного документооборота предприятия должна включать в себя семь подсистем: межсетевого экранирования, обнаружения вторжений, анализа

защищенности, криптографической защиты, активного мониторинга, антивирусной защиты и управления. Все они размещаются в ИС, которая функционально разделяется на следующие сегменты:

- сегмент почтовых серверов с размещенными в нем SMTP/POP3-серверами ИС. В данном сегменте устанавливаются серверные датчики подсистемы обнаружения вторжений, предназначенной для выявления и блокирования сетевых атак, а также датчики подсистемы антивирусной защиты, позволяющие обнаруживать враждебный код и удалять его из ИС;
- коммуникационный сегмент с коммутаторами и маршрутизаторами, а также с подсистемой межсетевого экранирования и сетевыми датчиками подсистемы обнаружения вторжений;
- административный сегмент управления безопасностью ИС с установленными в нем подсистемой анализа защищенности, позволяющей выполнять функции выявления уязвимостей в ПО ИС, и подсистемой централизованного управления всем комплексом средств защиты;
- сегменты локальных и удаленных пользователей ИС, в которых размещаются антивирусные датчики, специализированное ПО подсистемы криптографической защиты и датчики подсистемы активного мониторинга. Последние обеспечивают защиту от потенциальной утечки конфиденциальной информации через почтовую систему.

Система электронной почты является одним из важнейших компонентов электронного документооборота любого современного предприятия. Нарушение ее функционирования может привести к катастрофическим последствиям для последнего. Именно поэтому особое значение приобретает защита данной системы от потенциальных информационных атак, направленных на нарушение конфиденциальности, целостности и доступности передаваемой в ней информации. Только комплексный подход к решению этой задачи позволяет обеспечить высокий уровень информационной безопасности не только почтовой системы, но и всей КИС предприятия в целом.

5.5. Защита системы электронного документооборота DIRECTUM

На российском рынке систем электронного документооборота активно работают ряд ИТ-компаний. Основными потребителями систем электронного документооборота являются крупные российские компании. Сложная, географически распределенная структура этих компаний налагает определенный отпечаток на требования, предъявляемые к системам корпоративного электронного документооборота.

Наибольшей привлекательностью для крупных компаний обладают системы электронного документооборота, ориентированные на организацию удаленного доступа к ресурсам, т.е. имеющие Web-интерфейс и использующие мощную базу данных. Важным компонентом такой системы документооборота является электронная почта.

Прикладные решения для электронного документооборота, предложенные ИТ-компаниями, представлены в табл.5.3.

Таблица 5.3

Прикладные решения для электронного документооборота

Компания	Продукт	Назначение продукта
DIRECTUM	DIRECTUM 4.5	Система электронного документооборота и управления взаимодействием
Электронные офисные системы	Дело 8.9	Промышленная система автоматизации делопроизводства и электронного документооборота
Naumen	Naumen DMS 2.0	Автоматизация бизнес-процессов и документооборота в крупных компаниях
Cognitive Technologies	ЕВФРАТ-Документооборот 12.2	Комплексное решение для организации электронного документооборота
Евроменеджмент	Escom.doc 2.0.2	Автоматизация простых и сложных процессов документооборота
UpScale Soft	OPTiMA-workflow 1.19	Система конфиденциального электронного

		документооборота
ИнтерТраст	OfficeMedia R.5.5 и CompanyMedia R.3.3	Универсальная система электронного документооборота

Развитие российских разработок идет в соответствии с потребностью заказчиков автоматизировать максимальное количество бизнес-процессов и обеспечить единое информационное пространство. Это достигается за счет развития таких характеристик систем, как наличие полноценного хранилища контента, механизмы управления контентом, в том числе обеспечение полноценного процесса workflow с возможностью автоматизации специфических бизнес-процессов. Все это должно сочетаться с высокой масштабируемостью.

Система электронного документооборота и управления взаимодействием DIRECTUM 4.5, предлагаемая компанией Directum, удовлетворяет указанные потребности компаний-заказчиков и нацелена на повышение эффективности работы всех сотрудников организации в разных областях их совместной деятельности. Система DIRECTUM соответствует концепции Enterprise Content Management (ECM). Рассмотрим подробнее функциональные возможности и архитектуру системы DIRECTUM.

5.5.1. Функциональные возможности системы DIRECTUM

Система электронного документооборота DIRECTUM является полноценной ECM-системой (Enterprise Content Management) и поддерживает полный жизненный цикл управления документами, при этом традиционное «бумажное» делопроизводство органично вписывается в электронный документооборот [29].

DIRECTUM обеспечивает эффективную организацию и контроль деловых процессов на основе workflow: согласование документов, обработка сложных заказов, подготовка и проведение совещаний, поддержка цикла продаж и других процессов взаимодействия (рис.5.5).

Рис.5.5. Обобщенная схема реализации деловых процессов системой DIRECTUM

Решение указанных задач обеспечивают модули системы DIRECTUM:

- *управление электронными документами* - создание и хранение различных неструктурированных документов (тексты Microsoft Word, таблицы Microsoft Excel, схемы Microsoft Visio, рисунки CorelDraw, видео и пр.); расширенная поддержка версий документов и ЭЦП; структурирование документов по папкам; назначение прав доступа на документы; история работы с документами; полнотекстовый и атрибутивный поиск документов;
- *управление деловыми процессами* - поддержка процессов согласования и обработки документов на всех стадиях жизненного цикла (docflow); выдача электронных заданий и контроль их исполнения; взаимодействие между сотрудниками в ходе бизнес-процессов; поддержка свободных и жестких маршрутов; богатые расширяемые библиотеки блоков для формирования маршрутов (workflow);
- *управление договорами* - организация процесса согласования и регистрации договоров и сопутствующих документов, а также оперативной работы с ними (поиск, анализ, редактирование и т.д.);
- *управление совещаниями* - организация подготовки и проведения совещаний (согласование места и времени, состава участников, повестки); формирование и рассылка протокола; контроль исполнения решений совещания;

- *канцелярия* - регистрация бумажных документов в соответствии с требованиями Государственной системы документационного обеспечения управления (ГСДОУ); ведение номенклатуры дел с гибкими правилами нумерации; рассылка и контроль местонахождения бумажных документов; организация обмена электронными документами с ЭЦП с другими организациями;
- *управление взаимодействием с клиентами* - ведение единой базы организаций и контактных лиц; ведение истории встреч, звонков и переписки с клиентами; сопровождение процесса продаж в соответствии с регламентированными стадиями; планирование маркетинговых мероприятий; анализ эффективности продаж и маркетинговых воздействий.

5.5.2. Архитектура системы DIRECTUM

Система DIRECTUM имеет многоуровневую архитектуру. Архитектура служит гарантом доступности, надежности и безопасности системы, что позволяет системе DIRECTUM охватить всех компьютеризованных сотрудников и повысить эффективность работы организации в целом.

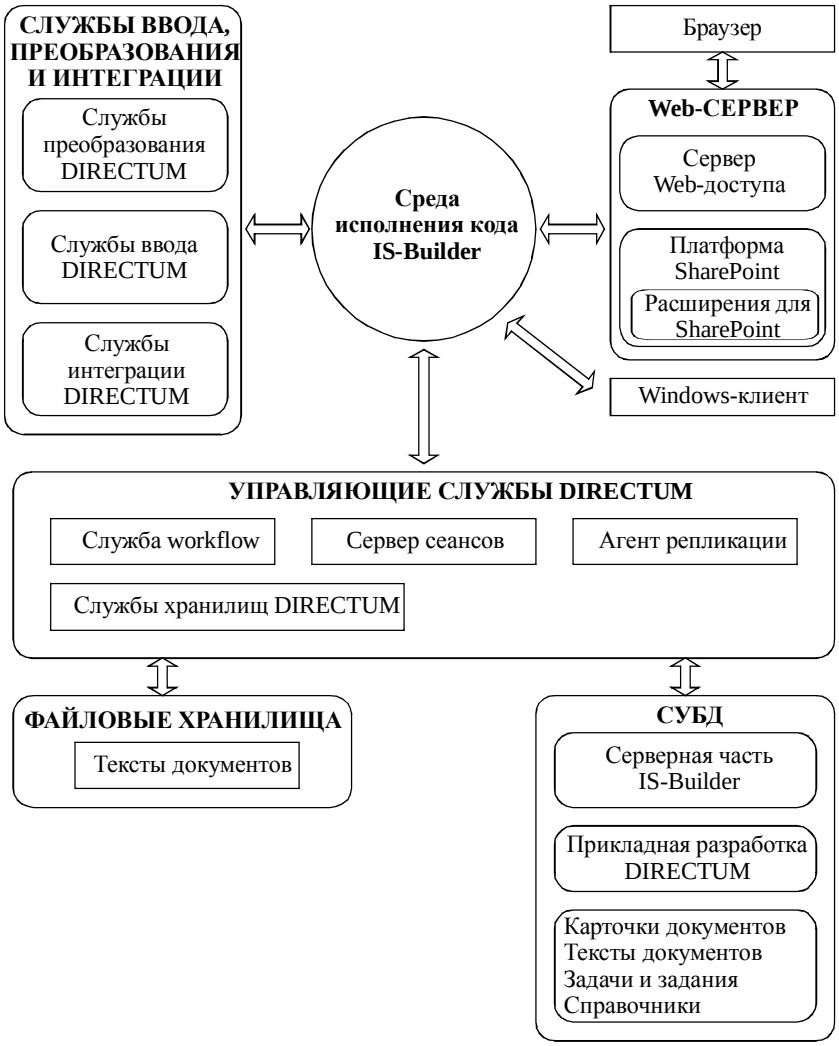

Рис.5.6. Архитектура системы DIRECTUM

Основными функциональными элементами архитектуры являются (рис.5.6):

- *СУБД* - хранилище данных и метаданных системы. Одним из важных компонентов системы, хранящихся в СУБД, является прикладная разработка DIRECTUM, которая определяет функциональность предметных модулей системы, заказных, а также разработанных партнерами;
- *управляющие службы DIRECTUM* - службы, обеспечивающие управление системой. Например, служба workflow управляет работой задач DIRECTUM, а DIRECTUM Storage Services отвечает за файловые хранилища документов. Все управляющие службы могут быть установлены как на один компьютер, так и на различные - в целях распределения нагрузки;
- *IS-Builder Runtime Environment* - среда исполнения кода, реализующая интерфейс служб и пользовательских приложений (в том числе сторонней разработки) для доступа к системе. В частности, сервер Web-доступа DIRECTUM, реализованный на платформе ASP.NET, использует IS-Builder Runtime

Environment для реализации всех функций системы, которые становятся доступны пользователям через Web-браузер;

- *клиенты системы DIRECTUM* - приложения для конечных пользователей, инструментарий разработки, утилиты администрирования системы. Клиентом может быть как Windows-приложение, использующее для доступа к системе IS-Builder Runtime Environment, так и Web-браузер;
- *файловые хранилища* - архивы больших или редко используемых документов, которые эффективнее держать за пределами СУБД; управляются собственными службами.

Архитектура системы DIRECTUM, являясь частью информационной инфраструктуры организации, имеет характеристики, важные для любой корпоративной системы:

- *открытость* - основа системы DIRECTUM - платформа IS-Builder - поддерживает технологии Microsoft COM и .NET. Она содержит готовые инструменты интеграции с корпоративными приложениями, в том числе набор функций для обработки XML-документов. Корпоративные стандарты и открытая структура данных позволяют интегрировать DIRECTUM в информационную инфраструктуру организации;
- *расширяемость* - как правило, в каждой организации выдвигают уникальные требования к построению электронного документооборота и решению задач взаимодействия. Объектная модель и предметно-ориентированный инструмент разработки IS-Builder позволяют создавать собственные и изменять существующие объекты для решения специфичных задач. Поскольку ядром системы является COM-сервер, управляющие функции системы можно использовать в любых сторонних приложениях;
- *масштабируемость* - выделение нескольких уровней архитектуры позволяет повышать производительность системы не только посредством наращивания мощности аппаратных средств, но и благодаря распределению служб по различным серверам. Механизм репликации IS-Builder позволяет построить территориально распределенную систему, минимизируя как требования к пропускной способности каналов связи за счет объема передаваемых данных между серверами, так и технические требования к вторичным серверам. Выделение как SQL-серверных, так и файловых хранилищ документов позволяет гибко управлять распределением нагрузки на серверы организации при доступе к документам;
- *надежность* - архитектура DIRECTUM поддерживает транзакционную модель, которая гарантирует целостность данных системы на протяжении всех стадий их жизненного цикла. Управляемые SQL- и файловые хранилища документов позволяют организовать надежное хранение документов;
- *безопасность* - для каждого объекта системы может быть задано, какие пользователи или группы имеют право выполнять с ним определенные действия.

Конфиденциальные электронные документы и задачи могут быть зашифрованы непосредственно в системе любым CryptoAPI-совместимым криптопровайдером (в том числе сертифицированным ФСБ), что гарантирует защиту даже от лиц, имеющих неограниченный доступ к данным. Протоколирование всех действий пользователя позволяет восстановить историю работы с объектами системы в случае нарушения режима безопасности. Обеспечивается надежная защита от несанкционированного доступа к хранилищам документов всех типов.

Возможности системы DIRECTUM существенно расширяются благодаря таким компонентам, как

- *предметно-ориентированный инструмент разработки IS-Builder* - модификация и разработка новых карточек электронных документов, справочников, отчетов, блоков типовых маршрутов; встроенный язык программирования ISBL; интеграция с другими системами;
- *службы файловых хранилищ (DIRECTUM Storage Services)* - управление хранением большого объема данных в единой системе; архивное хранение документов; работа с медиаданными; настройка политик хранения, обеспечивающих автоматическое перемещение данных по хранилищам;
- *сервер Web-доступа*. Работа с электронными документами, задачами и заданиями через Web-браузер;
- *расширения для SharePoint* - набор готовых Web-частей и интеграционных механизмов, обеспечивающих доступ к данным DIRECTUM из портала на базе Microsoft SharePoint;
- *сервер репликации* - создание территориально распределенных систем, обменивающихся данными в режиме off-line; иерархическая система вторичных серверов; настраиваемый состав реплицируемых данных;
- *DIRECTUM OverDoc* - просмотр, редактирование и подписание документов ЭЦП вне системы DIRECTUM для обмена между разными организациями; распространяется бесплатно;
- *технология быстрой идентификации документа DIRECTUM RapID* - маркировка документа штрих-кодом и быстрый поиск электронного документа по его бумажной копии;
- *службы ввода документов (DIRECTUM Capture Services)* - массовый ввод документов в DIRECTUM с различных источников (сканеров, многофункциональных устройств (МФУ), которые могут объединять в одном аппарате функции принтера, ксерокса, сканера и др., файловой системы, факсов, электронной почты и т.д.);
- *службы преобразования документов (DIRECTUM Transformation Services)* - преобразование документов в другие форматы, извлечение из документов полезной информации;

- *набор средств интеграции (DIRECTUM Integration Toolset)* - легкая интеграция с ERP-системами: двухсторонняя синхронизация справочников, включение объектов системы в workflow, генерация документов и доступ к ним из ERP-системы.

Архитектура системы DIRECTUM позволяет создавать масштабируемые, надежные и безопасные корпоративные решения для управления документами, бизнес-процессами, совещаниями, договорами и взаимодействием с клиентами.

Адаптация системы DIRECTUM к специфическим нуждам организации и развитие системы вместе с ростом потребностей бизнеса обеспечивается возможностями инструмента разработки IS-Builder, который предлагает развитые средства быстрого и удобного создания новых справочников, карточек электронных документов, сценариев, экранных форм, типовых маршрутов, их отдельных блоков и других компонентов корпоративной системы электронного документооборота.

Интеграция системы DIRECTUM с ERP-системами, корпоративными порталами и другими составными частями ИТ-инфраструктуры организации возможна по различным направлениям благодаря развитым интеграционным возможностям платформы DIRECTUM на базе набора средств интеграции DIRECTUM Integration Toolset и открытой архитектуре.

Территориально распределенная работа крупных организаций поддерживается сервером репликации, который обеспечивает прозрачный для пользователей и разработчика обмен данными - документами, задачами, заданиями, справочниками - между подразделениями организации.

Работа с DIRECTUM через Интернет и в Интранет реализована в DIRECTUM по нескольким направлениям. Сервер Web-доступа обеспечивает работу пользователей с документами и задачами DIRECTUM через интерфейс браузера, а расширения DIRECTUM для SharePoint предлагают специализированный интерфейс доступа к данным системы DIRECTUM через корпоративный портал.

Обмен документами между сторонними организациями возможен благодаря специальным механизмам DIRECTUM, позволяющим передавать и контролировать доставку официальной корреспонденции в электронном виде на основе отраслевого формата обмена электронными документами.

Обмен электронными документами между организациями-партнерами, даже в случае отсутствия системы электронного документооборота у любой из сторон, возможен с помощью бесплатной программы DIRECTUM OverDoc на основе специально разработанного формата структурированного электронного документа.

Инструменты администрирования DIRECTUM позволяют управлять всеми задачами администрирования - от регистрации пользователей до создания политик миграции документов между файловыми хранилищами.

В связи с ограниченным объемом книги рассмотрим подробнее работу одного из основных модулей системы DIRECTUM - «Управление электронными документами».

5.5.3. Управление электронными документами в системе DIRECTUM

Постоянное увеличение объема накапливаемых в организации документов (приказов, писем, договоров, служебных записок, инструкций и т.д.) приводит к увеличению объема трудно решаемых задач: поиск документов, поддержание их в актуальном состоянии, обеспечение режима конфиденциальности и сохранности документов и т.д. В результате возникает ситуация информационной недостаточности, управленческие решения принимаются не оперативно, а управленческие затраты на документооборот увеличиваются. Все это негативно сказывается на эффективности работы организации в целом.

Для решения указанных задач в системе DIRECTUM выделен модуль «Управление электронными документами», с помощью которого все сотрудники организации работают с документами преимущественно в электронном виде. Модуль обеспечивает создание, хранение, поиск, изменение различных неструктурированных документов (тексты Microsoft Word, электронные таблицы Microsoft Excel, рисунки Visio и CorelDraw, звуки, видео и пр.).

Одно из основных понятий, используемых в системе DIRECTUM, - *электронный документ*. Каждый электронный документ состоит из *текста* - содержимого электронного документа, и *карточки* - формы, содержащей набор атрибутов, описывающих документ (автор, тип документа, дата создания, корреспондент и т.д.), которые могут быть использованы для поиска и группировки электронных документов. Для организации хранения документов используются *папки*, в которые помещаются *ссылки* на электронные документы и другие папки.

Каждый документ может иметь неограниченное количество *версий*, при этом версии одного и того же документа могут быть в разных форматах (например, DOC и PDF). Для каждого вида документа (договоры, счета и пр.) определяется свой *жизненный цикл*, автоматически изменяющий состояние документа в ходе работы с ним.

Модуль использует возможности файловых хранилищ для организации работы с документами большого объема, а также для создания долговременного архива электронных документов.

Ввод и преобразование документов. Внедрение системы электронного документооборота позволяет значительно сократить объем бумажных документов. Тем не менее, полностью исключить бумагу и перейти на электронную документацию невозможно, так как правовые нормы до сих пор требуют наличия бумажной документации, а значительная часть информации поступает в компанию не в электронном виде.

Для облегчения ввода информации с различных носителей в системе DIRECTUM предусмотрены службы ввода документов DIRECTUM Capture Services (рис.5.7).

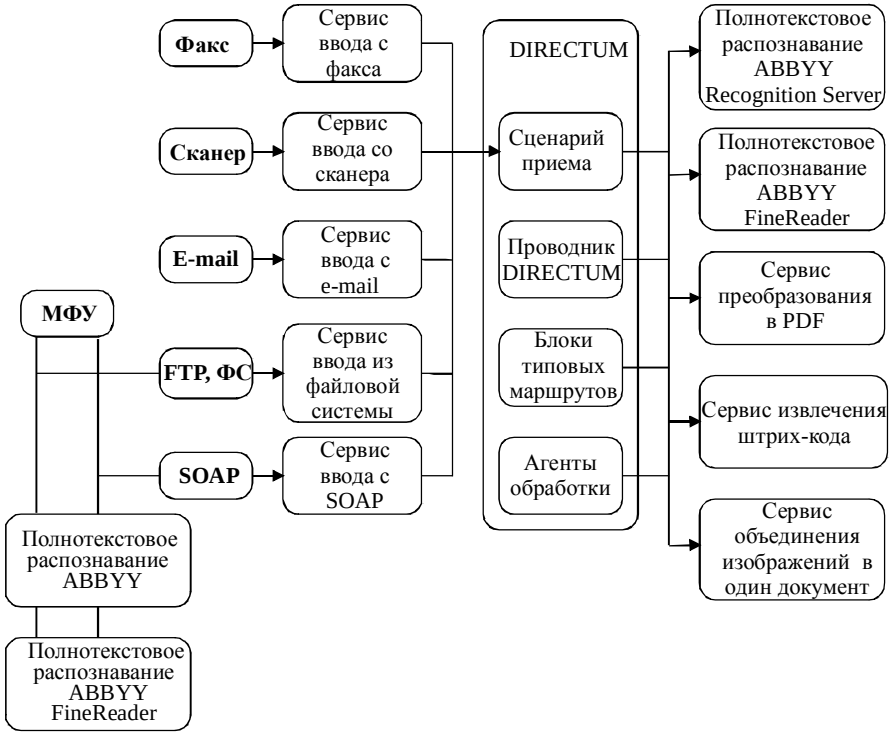

Рис.5.7. Службы ввода документов в системе DIRECTUM

Службы обеспечивают массовый ввод документов со сканеров, МФУ («сендеров»), папок файловых систем, факсов и т.д.

Службы включают в себя специальные сервисы по интеграции с оборудованием и захвату образов документов:

- сервис ввода с потокового сканера;
- сервис ввода с факса;
- сервис ввода из файловой системы;
- сервис извлечения штрих-кода;
- сервис группировки изображений.

DIRECTUM Capture Services также реализуют первичную обработку документов, например разделение потока страниц по разным признакам - наличию и типу штрих-кода, белому листу, количеству страниц и т.д.

Дальнейшая обработка занесенных в систему документов может осуществляться службами преобразования документов DIRECTUM Transformation Services, которые переводят документы в другие форматы (в частности, в формат PDF) и извлекают из них необходимую информацию.

Организация хранения документов. Хранение документов в системе DIRECTUM организовано таким образом, чтобы обеспечить удобство работы пользователей и гарантировать сохранность, конфиденциальность и быстрый поиск документов. Размещение всех документов в едином информационном пространстве системы DIRECTUM избавляет каждого пользователя от проблемы поиска документов, созданных другими пользователями в локальных каталогах на своих компьютерах, и от проблемы доступа к таким документам. При этом каждый пользователь системы DIRECTUM может организовать удобную лично ему, иерархию папок, куда помещается не сам документ, а ссылка на него. В результате один документ может «лежать» в нескольких папках, а может «не лежать» ни в одной папке, находясь только в хранилище DIRECTUM.

Службы файловых хранилищ DIRECTUM Storage Services позволяют хранить документы как в базе данных SQL-сервера, отличающегося простотой администрирования и высокой производительностью, так и в файловых хранилищах, что практически неограниченно расширяет доступное для хранения документов пространство и обеспечивает потоковый доступ (рис.5.8).

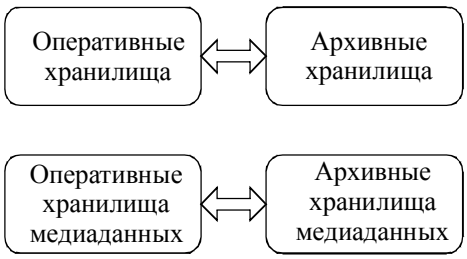

Рис.5.8. Файловые хранилища системы DIRECTUM

Возможности поиска документов. В системе DIRECTUM предусмотрены различные возможности для оперативного поиска документов. Поиск может осуществляться по заданным реквизитам карточки, а также по содержимому документа с учетом всех грамматических форм слов на основе морфологического анализа (полнотекстовый поиск).

В системе имеется возможность осуществлять специализированный поиск электронных документов, используя:

- предопределенные поиски (например, «Мои последние измененные документы»);
- дополнительные поиски по часто используемым критериям, специально настроенные администраторами;
- возможность задания для любого документа связанных с ним по смыслу или логике документов и перехода от одного связанного документа к другому, включая его собственные связанные документы.

Кроме того, в системе каждый пользователь может создать папки поиска. Для таких папок определяются критерии поиска, по которым формируется содержимое папки. При этом содержимое папки актуализируется при каждом ее открытии.

Для поиска документов по бумажному аналогу используется технология быстрой идентификации документа DIRECTUM Rapid Document Identification (RapID). Используя маркировку бумажных аналогов документов уникальным штрих-кодом и применяя в дальнейшем сканер штрих-кодов, пользователи могут найти электронный документ в системе оперативно и безошибочно. Штрих-код позволяет однозначно идентифицировать документы и исключить ошибки, вызванные несовпадением электронного и бумажного документов. При сканировании штрих-кода документ открывается в специальном, удобном пользовательском интерфейсе, облегчающем работу руководителей и делопроизводителей.

Работа с содержанием документа. Система DIRECTUM позволяет использовать любые программы для создания и редактирования электронных документов (Microsoft Word, Microsoft Excel, Microsoft Project, Microsoft Visio, AutoCAD, CorelDraw и др.).

Для оперативного создания однотипных электронных документов используются шаблоны, определяющие начальное содержимое документа. Например, шаблоны «Исходящее письмо», «Договор поставки», «Коммерческое предложение» и т.п. При этом в текст документа могут автоматически подставляться поля, заполненные в карточке документа.

Функция импорта документов позволяет легко занести документ в систему из любого файла операционной системы, а также непосредственно со сканера. Документ также может быть занесен в систему из электронного письма, благодаря интеграции DIRECTUM с Microsoft Outlook.

Интеграция с Microsoft Word, Microsoft Excel, Microsoft Project, а также с бесплатно распространяемым пакетом офисных приложений OpenOffice.org позволяет непосредственно из приложения отправлять документ на согласование, смотреть историю работы с документом и связанные документы, вставлять штрих-код и сравнивать версии документов.

Жизненный цикл и версии документа. Каждый документ в системе DIRECTUM может иметь неограниченное количество версий. Это позволяет хранить историю изменения содержания документа (например, в процессе согласования) и избегать работы с устаревшей информацией. При этом версии одного и того же документа могут быть в разных форматах, что облегчает поиск, хранение и доступ к документу и значительно повышает удобство работы пользователей. Например, версии, возникающие в процессе разработки и согласования, могут храниться в удобном для редактирования формате DOC, а окончательная согласованная версия - в неизменяемом формате PDF.

Версия электронного документа отражает актуальность его содержимого. Каждая версия может находиться в одном из состояний: в разработке, действующая, устаревшая. Для визуального представления состояния версии используется особое начертание шрифта. Для каждого вида документа (договоры, счета и пр.) предусматривается свой жизненный цикл, в котором задаются стадии жизненного цикла и правила перехода между ними. Переход между стадиями может осуществляться автоматически. Например, жизненный цикл вида документа «Входящий счет на оплату» включает стадии «Инициализация», «Внутреннее согласование», «Отказано в оплате», «Оплата», «Оплачен». В процессе работы с документом в модуле «Управление деловыми процессами» стадии будут автоматически меняться, соответственно изменяя состояние документа и его визуальное представление в системе. Управление жизненным циклом документа осуществляется при помощи удобного графического редактора.

Обеспечение конфиденциальности документов. Одной из важнейших функциональных задач системы DIRECTUM является защита информации от несанкционированного доступа. Конфиденциальность документов, хранящихся в системе DIRECTUM, обеспечивается следующими возможностями:

- контроль и настройка прав доступа на любой объект системы (полный доступ, изменение, просмотр, полное отсутствие доступа), обеспечивающие защиту от несанкционированного доступа;
- шифрование электронных документов, позволяющее дополнительно защитить текст электронного документа, в том числе от пользователей со статусом «администратор»; шифрование может осуществляться как на основе сертификата закрытого ключа пользователя (хранимого в том числе на переносном ключе), так и установкой обычного пароля;
- протоколирование всех действий пользователей, позволяющее быстро восстановить историю работы с документом и проконтролировать такие действия над документом, как просмотр, изменение, экспорт копии документа и пр.

Для предотвращения прямого доступа к текстам документов, минуя систему DIRECTUM, реализованы специальные средства защиты как файловых хранилищ, так и хранилищ на SQL-сервере.

Использование электронной цифровой подписи. ЭЦП позволяет заменить традиционные печать и подпись, гарантируя авторство и неизменность документа после его подписания. С помощью ЭЦП можно подписать любую версию электронного документа, фиксируя и сохраняя информацию о том, кто и когда поставил подпись.

Система DIRECTUM поддерживает два вида ЭЦП: визирующую и утверждающую. *Визирующая подпись* свидетельствует о том, что подписавший документ ознакомился с ним (завизировал его).

Утверждающая подпись может быть поставлена ограниченным кругом лиц в рамках заданных полномочий и свидетельствует об окончательном утверждении документа. Подпись любого вида, поставленная на версии документа, защищает ее от изменений.

Надежность работы с ЭЦП в системе DIRECTUM обеспечивает использование переносных ключей (USB-ключи, смарт-карты), позволяющих хранить персональный ключ пользователя не на общедоступном компьютере, а на индивидуальном носителе. Для повышения надежности работы с ЭЦП система DIRECTUM может быть интегрирована с различными системами криптозащиты информации, в том числе сертифицированными ФСБ (ФАПСИ), благодаря реализации ЭЦП с использованием Microsoft CryptoAPI.

Организация коллективной работы с документами. При одновременной работе большого количества пользователей в едином информационном пространстве возникает проблема одновременного редактирования одного документа несколькими пользователями. Для решения этой задачи в системе DIRECTUM предусмотрен специальный механизм блокировок. Благодаря ему пользователи могут одновременно редактировать разные версии документа и карточку, а также создавать новые версии, в том числе в разных форматах. При этом остальные пользователи могут просматривать редактируемые версии и карточку документа. Автоматически создаваемые теневые копии документа позволяют вернуться к случайно удаленному или некорректно измененному содержимому документа.

В системе существует возможность получения оповещений об освобождении документа, если при попытке открытия этот документ был уже заблокирован другим пользователем. Это позволяет быстро вернуться к документу сразу после того, как другой пользователь освободит его.

Система DIRECTUM позволяет также работать с отдельными документами в автономном режиме (например, забрать файл домой, поработать, потом возвратить). Для этого существуют возможности экспорта документа из системы и импорта документа в систему, а также возможность блокировки экспортированного документа до тех пор, пока не будет произведен его возврат в систему. Экспорт документа также возможен не только в оригинальный формат, но и в ZIP-архив, в PDF, а также в специально разработанный открытый формат структурированного электронного документа (ESD).

ESD-документ содержит все атрибуты карточки и электронные подписи, т.е. сохраняет юридическую значимость документа и может быть использован для взаимодействия со сторонними организациями. Работа с ESD-документом ведется с помощью свободно распространяемой программы DIRECTUM OverDoc.

Таким образом, система DIRECTUM поддерживает полный комплекс работ с электронными документами, обеспечивая:

- соблюдение режима конфиденциальности доступа к документам;
- применение электронной цифровой подписи;
- надежное хранение документов, в том числе в разных форматах;
- реализацию защищенного электронного документооборота между организациями и т.д.

Вопросы для самоконтроля

1. Укажите преимущества электронного документооборота по сравнению с бумажным документооборотом. Укажите различия между понятиями «система электронного документооборота» (СЭД) и ECM (Enterprise Content Management).
2. Охарактеризуйте базовые составляющие системы электронного документооборота.

3. Опишите функциональность подсистемы автоматизации управления потоками работ (WorkFlow).

4. Укажите особенности построения и функционирования системы распределенного электронного документооборота.

5. Назовите угрозы информационной безопасности для СЭД и охарактеризуйте источники этих угроз.

6. Какие функции должны быть реализованы средствами защиты информации СЭД?

7. Назовите основные угрозы информационной безопасности баз данных. Укажите методы и средства защиты СУБД.

8. Определите понятие «RAID-массив». Поясните особенности применения RAID-массивов в СУБД.

9. Сравните возможности средств защиты СУБД Microsoft Access и СУБД Oracle.

10. Охарактеризуйте методы и средства защиты корпоративного почтового документооборота.

11. Опишите функциональные возможности и архитектуру системы электронного документооборота DIRECTUM.

12. Охарактеризуйте приемы и методы защиты, реализованные в системе DIRECTUM.

Часть 3. КОМПЛЕКСНАЯ ЗАЩИТА КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Корпоративные информационные системы становятся одним из главных инструментов управления бизнесом современной компании. При этом эффективное 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 комплексной защиты информации внедрение информационных технологий может оказаться экономически невыгодным в результате значительного ущерба из-за потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях.

Глава 6. Принципы комплексной защиты корпоративной информации

Один только разум может
обеспечить безмятежный покой.

Сенека. «Письма»

При создании системы защиты корпоративной информации необходимо использовать принцип глубоко эшелонированной обороны от внешних и внутренних угроз. Эта стратегия предполагает необходимость создания многоуровневой системы защиты, при которой прорыв одного уровня защиты не означает прорыва всей системы безопасности. Комплексный подход к построению системы защиты информации позволяет организовать целостную систему защиты от угроз.

6.1. Архитектура корпоративной информационной системы

Информационные системы повышенной сложности, такие, как КИС, как правило, состоят из нескольких подсистем, решающих конкретные задачи. При построении КИС следует увязывать подсистемы в единый комплекс, придерживаясь ряда основополагающих принципов:

- использование общепринятых стандартов, поддерживаемых основными фирмами-производителями программного обеспечения;
- применение программного обеспечения достаточной производительности, чтобы его не менять при увеличении мощности и количества используемого оборудования. Это качество называется масштабируемостью программного обеспечения;
- соблюдение принципа многозвенности, означающего, что каждый уровень системы (клиент, Web-сервер, сервер приложений, сервер баз данных) реализует функции, наиболее ему присущие;
- реализация принципа аппаратно-платформенной независимости и системного программного обеспечения;
- осуществление принципа коммуникативности, когда различные уровни системы могут взаимодействовать между собой как по данным, так и по приложениям [9].

В настоящее время наиболее подходящими технологиями для построения КИС являются Экстранет и Интранет, предусматривающие специфические решения для приложений архитектуры клиент - сервер, с использованием всего многообразия технологий и протоколов, разработанных для глобальной сети Интернет. Имеются в виду, в частности, применение:

- в качестве транспортного протокола - TCP/IP;
- встроенных средств защиты и аутентификации;
- технологии WWW в архитектуре «клиент - Web-сервер - сервер приложений - сервер баз данных» при разработке приложений [1, 9].

Вместе с тем Web-технологии при всех своих значительных преимуществах вносят и новые проблемы, связанные с масштабируемостью, управлением сеансами и состоянием сети, ее защитой и возможными изменениями стандартов. Большие нагрузки от пользователей требуют высокоэффективной архитектуры аппаратной и программной платформы, которая должна допускать масштабируемость ресурсов. Управление ресурсами и разграничение доступа, как правило, ориентированы на отдельный WWW-сервер и не охватывают все множество информационных ресурсов корпорации.

Становятся первостепенными проблемы защиты, когда компании делают внутренние базы данных доступными для внешних пользователей. Установление подлинности пользователей и безопасность передачи данных превращается в большую проблему в Web-среде из-за большого количества потенциально анонимных пользователей.

Что касается стандартов, то технологии WWW все еще изменяются и стандарты еще не сформировались. Например, сейчас происходит расширение HTML языком описания Web-документов XML.

Важнейшими вопросами при реализации КИС на базе технологий Интернет/Интранет являются организация защиты информации, централизованного управления информационными ресурсами, разграничение доступа к ресурсам. Особенно это важно для доступа пользователей из внешних сетей к ресурсам КИС. Это так называемая Экстранет-технология.

Общепринятым подходом к решению вопросов защиты является использование в корпоративной сети, имеющей выход в публичную сеть Интернет, следующей стратегии управления доступом между двумя сетями:

- весь трафик, как из внутренней сети во внешний мир, так и наоборот, должен контролироваться корпоративной системой;
- через систему может пройти только авторизованный трафик, который определяется стратегией защиты.

Межсетевой экран - это механизм, используемый для защиты доверенной сети (внутренняя сеть организации) от сети, не имеющей доверия, например Интернет.

Несмотря на то что большинство МЭ в настоящее время развернуто между Интернет и внутренними сетями (Интранет), имеет смысл использовать их в любой сети, базирующейся на технологии Интернет, скажем, в распределенной сети предприятия.

Перечисленные принципы построения учтены в структурной схеме корпоративной информационной системы, представленной на рис.6.1.

Рис.6.1. Структурная схема корпоративной информационной системы

В этой структурной схеме можно выделить такие виды управления, как

- централизованное управление всей системой предприятия;
- управление подразделениями, приложениями и серверами;
- управление всей сетью;
- управление конечными пользователями [9].

Эти четыре уровня управления КИС могут служить объектами угроз для информационной безопасности предприятия.

Соответственно система информационной безопасности КИС должна включать в себя защиту:

- централизованного управления;
- приложений и соответствующих серверов;
- сети;
- конечных пользователей.

Наличие большого числа информационных и вычислительных ресурсов (баз данных и приложений), используемых на предприятии и функционирующих на различных аппаратных и программных платформах, делает актуальной задачу создания и внедрения системы санкционированного доступа к единому информационному пространству предприятия. Осуществление подобного санкционированного доступа возможно при условии:

- обеспечения соответствующего единого механизма;
- единой политики безопасности и защиты информации;
- централизованного и непрерывного контроля за использованием ресурсов и управлением ими.

При этом обязательно должно быть учтено наличие большого числа наследуемых приложений, исторически используемых на том или ином предприятии. Возможная схема санкционированного доступа к информационным ресурсам предприятия представлена на рис.6.2.

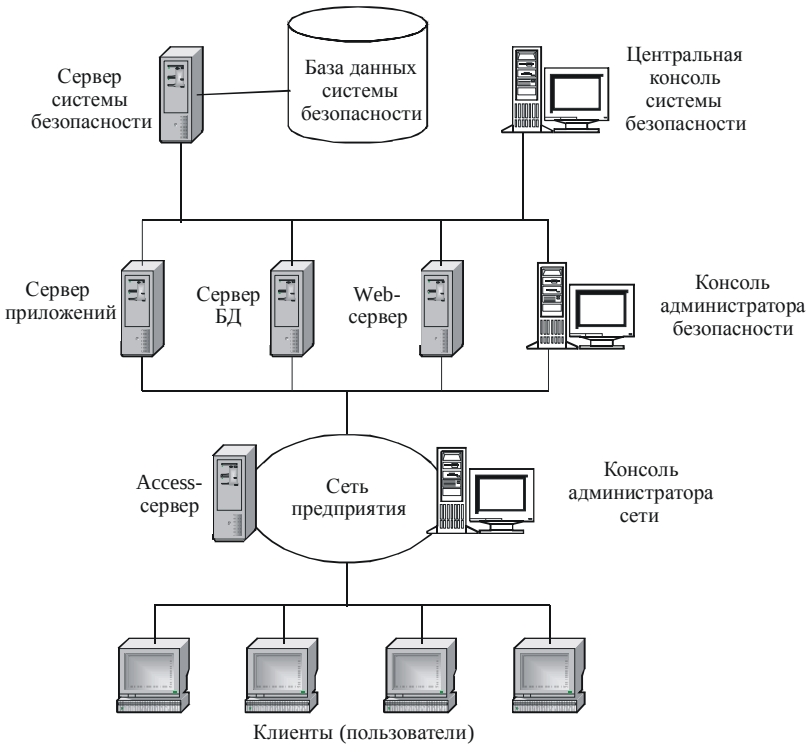

Рис.6.2. Структурная схема санкционированного доступа к информационным ресурсам предприятия

На схеме представлена многозвенная архитектура, состоящая из:

- клиентского уровня - терминальных компьютеров пользователей под управлением ОС MS Windows NT/2000/XP, использующих один из широко распространенных браузеров: Microsoft Internet Explorer или Netscape Navigator;
- уровня серверов доступа (access server) - специализированных серверов приложений, реализующих функции аутентификации пользователей, управления правами доступа к ресурсам интегрированной информационной системы управления предприятием (ИИСУП) (распределенный каталог), контроля и протоколирования сеансов, доступа к информационным и вычислительным ресурсам ИИСУП;
- уровня серверов приложений - масштабируемой структуры серверов, обеспечивающих унифицированные средства представления информации и функционирования подсистем ИИСУП;
- уровня серверов баз данных;
- уровня Web-серверов.

6.2. Структура системы защиты информации в корпоративной информационной системе

Одной из существенных особенностей КИС является реализация в ней принципа централизованного управления, благодаря чему возможно выполнение таких важных функций, как

- авторизация и управление распределенной информацией в масштабах всего предприятия;
- возможность централизованной аутентификации и управление контролем доступа ко всем Web-серверам вне зависимости от их платформ (централизованное управление Web-пространством за счет связи Web-серверов в одно логическое Web-пространство);
- управление доступом к персональной информации потребителей;
- централизованное кроссплатформенное управление учетными записями пользователей;
- управление цифровыми сертификатами для электронного бизнеса;
- централизованное кроссплатформенное управление доступом пользователей к информационным ресурсам;
- управление рисками на предприятии, позволяющее системным администраторам контролировать все несанкционированные вторжения на предприятие [9, 19].

Предприниматели постоянно сталкиваются с увеличивающимися рисками от вирусных атак, несанкционированного доступа, а также с атаками по блокированию программно-технического обеспечения предприятия. Противостоять всем внутренним и внешним (из Интернет) угрозам можно лишь с помощью соответствующей эффективной защиты предприятия. Лучшей ее разновидностью является управление рисками предприятия, когда к его менеджерам своевременно и в необходимых объемах поступает из различных контрольных точек системы безопасности предприятия информация, необходимая для управляющих воздействий.

Управление рисками предприятия обеспечивается с использованием централизованного пульта (консоли) безопасности предприятия. С его помощью фиксируются, контролируются и устраняются аварийные события на всем предприятии. Этот пульт позволяет осуществлять управление угрозами и уязвимостью по всему предприятию, а также гарантировать доступ к сетям, системам, приложениям и рабочим столам, совместимый с политикой защиты предприятия [1].

Управляя рисками предприятия, системные администраторы могут:

- точно идентифицировать различные типы угроз и нападений, используя современную технику корреляций, что очень важно для быстрого ответа по защите предприятия;
- обеспечивать средствами поддержки принятие решений, позволяющих организациям осуществлять профилактические меры по сокращению деловых рисков. Располагая подобными средствами, администраторы по безопасности могут точно определять уязвимые «горячие точки» (hotspots) и осуществлять корректирующие действия, модернизирующие их политику защиты;
- быстро принимать решения по защите от атак по блокированию программно-технического обеспечения, от вирусов или несанкционированного доступа. Меры, предлагаемые в таких случаях, включают в себя нередко реконфигурирование межсетевых экранов, аннулирующее учетные записи пользователя на серверах и удаляющее вирусы с персональных компьютеров.

Управление рисками предприятия вполне согласуется с идеологией неоднородной технологии безопасности разнообразных компьютерных программ. В итоге формируется всестороннее управление информационной безопасностью предприятия.

Подобный принцип управления безопасностью предприятия уже существует и представляет собой открытую, базирующуюся на стандартах, кроссплатформенную систему, позволяющую эффективно бороться с вторжениями и безопасно управлять уязвимостью в сетях, хостах, операционных системах, приложениях, серверах и настольных компьютерах. В этом случае структурная схема системы защиты информации КИС может быть представлена в виде, показанном на рис.6.3, где слева указаны уровни защиты информации КИС [9].

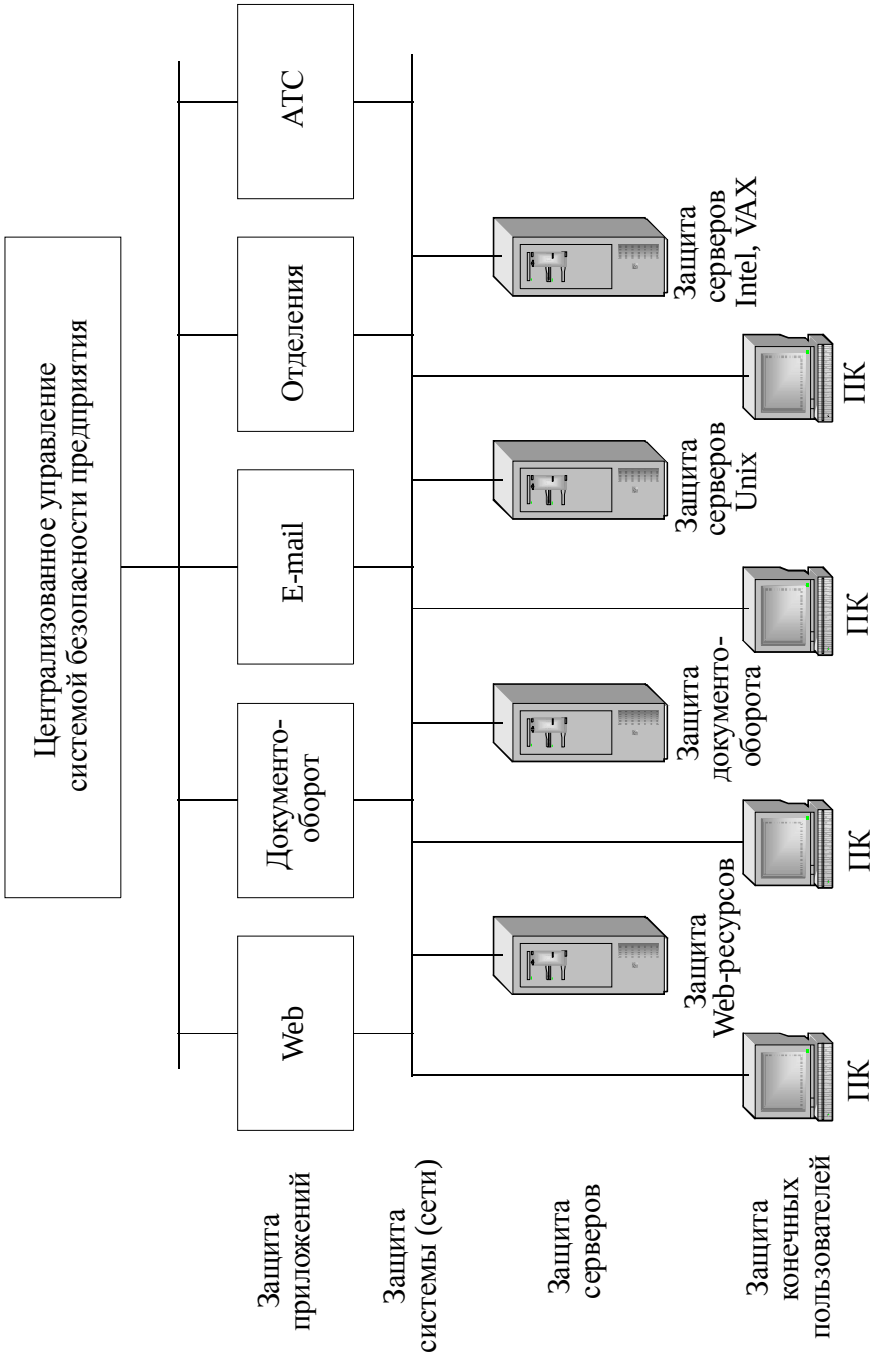

Рис.6.3. Структурная схема системы защиты информации корпоративной информационной системы

Функции уровней защиты могут быть сформулированы следующим образом.

Централизованное управление рисками и администрирование системы безопасности:

- Централизованное администрирование.
- Административный контроль полномочий главным администратором.
- Делегирование части полномочий младшим администраторам отдельных ресурсов.
- Управление событиями.
- Принятие решений по управлению рисками.
- Связь с централизованной консолью управления предприятием.
- Долговременное хранение статистики тревог и вторжений.
- Управление атрибутами пользователей (учетными записями пользователей) и обслуживание пользователей в распределенных сетях.
- Осуществление централизованной аутентификации и управления контролем доступа ко всем Web-серверам вне зависимости от их платформ.

- Обеспечение консолью центрального управления службой безопасности:

- управление пользователями (группами и ролями в полной сети предприятия);
- управление директориями;
- управление пользовательскими привилегиями;
- делегирования части административных полномочий младшим администраторам;
- управление набором ресурсов и распределение администрирования между младшими администраторами.

При этом сама консоль должна позволять отделять управление разработкой политики безопасности от ее реализации.

Защита управления приложениями:

- Защита доступа к ресурсам приложений.
- Установление и контроль связи учетных записей пользователя с различными типами ресурсов (файлов, директорий, принтеров, приложений и др.).
- Возможность делегирования управления доступа к ресурсам младшим администраторам при высокой степени контроля.
- Установление и контроль групповых подсоединений пользователей к ресурсам.
- Использование общего административного интерфейса доступа пользователя к ресурсам системы.
- Возможность администрирования доступа к ресурсам на правилах, устанавливаемых ролями.
- Запрещение неправомочного доступа к информационным ресурсам и критическим сервисам.
- Управление аудитом.

Защита системы сетей:

- Защита внутрисетевого обмена (локальные вычислительные сети, Интранет).
- Защита межсетевого обмена (глобальные вычислительные сети, Экстранет).
- Защита обмена через Интернет.
- Осуществление стыковочных узлов, репликация доступа к ресурсам.
- Осуществление поддержки любых соединений (back-end), Web-серверов и поддержки соединений с ресурсами.
- Осуществление распределения нагрузки для улучшения производительности и восстановления после сбоев.

Защита конечных пользователей:

- Установление соответствия имени и пароля.
- Управление доступом с помощью списков контроля за пользователями, а также соответствующих правил обращения пользователей с информацией.
- Сертификация открытых ключей (Public Key Infrastructure).
- Поддержка статических и динамических ролей (например, доступ для чтения/записи, доступ только для чтения).
- Контроль попыток доступа к ресурсам и регистрация (обнаружение угрозы безопасности).
- Контроль соблюдения требований политики секретности.

6.3. Комплексный подход к обеспечению информационной безопасности КИС

При разработке архитектуры комплексной системы защиты информации необходимо учитывать следующие общие требования:

- информационная безопасность (ИБ) должна быть обеспечена на всех уровнях информационной системы: на организационно-управленческом, технологическом и техническом;
- ИБ должна быть обеспечена на всех стадиях жизненного цикла информационных систем;
- архитектура КСЗИ должна иметь распределенную и многоуровневую структуру, соответствующую структуре информационной системы;
- решения, образующие КСЗИ, должны выбираться с учетом принципа масштабируемости и модульного принципа построения, обеспечивающих наращивание и модернизацию подсистем по мере изменения требований к обеспечению ИБ, возникновения новых угроз, создания новых средств защиты и их модернизации;
- внедрение мер безопасности должно осуществляться в рамках всей инфраструктуры (а не только на критичных ресурсах);

- КСЗИ должна охватывать все этапы обработки информации (создание, сбор, обработка, накопление, хранение, поиск, распространение и использование информации) и не налагать жестких ограничений на используемые технологии построения информационных систем;
- КСЗИ должна быть интегрирована со встроенными средствами защиты информации прикладных систем, операционных систем и информационных сервисов.

Комплексная система защиты информации основана на совместном применении следующих мер и средств защиты:

- централизованное управление компонентами КСЗИ и мониторинг сетевой активности;
- использование пакетных фильтров и межсетевого экранирования уровня приложений для разграничения доступа пользователей к ресурсам Интернет и защиты внутренних ресурсов КИС от НСД из Интернет;
- применение разрешительного порядка предоставления пользователям привилегий доступа к ресурсам Интернет;
- обнаружение вторжений на сетевом и прикладном уровнях с соответствующей динамической реакцией на эти атаки, например, путем автоматического переконфигурирования межсетевых экранов и обрыва межсетевых соединений;
- обеспечение антивирусной проверки и удаление вирусов в проходящем из/в интернет-трафике электронной почты, FTP- и HTTP-трафике;
- гибкая организация демилитаризованных зон и возможности дополнительной защиты критических демилитаризованных зон.
- обеспечение отказоустойчивости и надежности корпоративной сети благодаря:

- дублированию каналов доступа в Интернет и каналов КИС,

- разнесению точек выхода из Интернет по различным траекториям,

- использованию протоколов динамического изменения топологии сети, прозрачному для пользователей,

- дублированию средств управления КСЗИ;

- эшелонирование защиты:

- последовательное размещение пакетных фильтров и межсетевых экранов уровня приложений, использование дополнительных межсетевых экранов для защиты критичных ресурсов,

- многоуровневое размещение средств обнаружения вторжений для контроля несанкционированной активности как перед межсетевыми экранами, так и за ними, а также обнаружение атак на межсетевые экраны изнутри КИС;

- централизованный аудит и формирование отчетов о сетевой активности и несанкционированных действиях;
- обеспечение целостности ресурсов КСЗИ и управляющего трафика КСЗИ с помощью штатных средств компонент КСЗИ;
- обеспечение централизованного контроля за уязвимостью компонент подсистем защиты.

Комплексная система защиты информации представляет собой целостный и достаточный набор средств защиты от актуальных угроз ИБ, который интегрируется в защищаемую информационную систему [19].

Общая структура комплексной системы защиты информации КИС показана на рис.6.4.

В состав КСЗИ обычно входят следующие подсистемы информационной безопасности:

- криптографическая защита и PKI;
- управление идентификацией и доступом;
- обеспечение безопасности коммутируемой инфраструктуры и беспроводных сетей;
- управление средствами защиты информации;
- контроль использования информационных ресурсов;
- межсетевое экранирование;
- обнаружение и предотвращение вторжений;
- защита от вредоносного кода и нежелательной корреспонденции;
- контроль эффективности защиты информации;
- мониторинг и управление инцидентами ИБ;
- обеспечение непрерывности функционирования средств защиты.

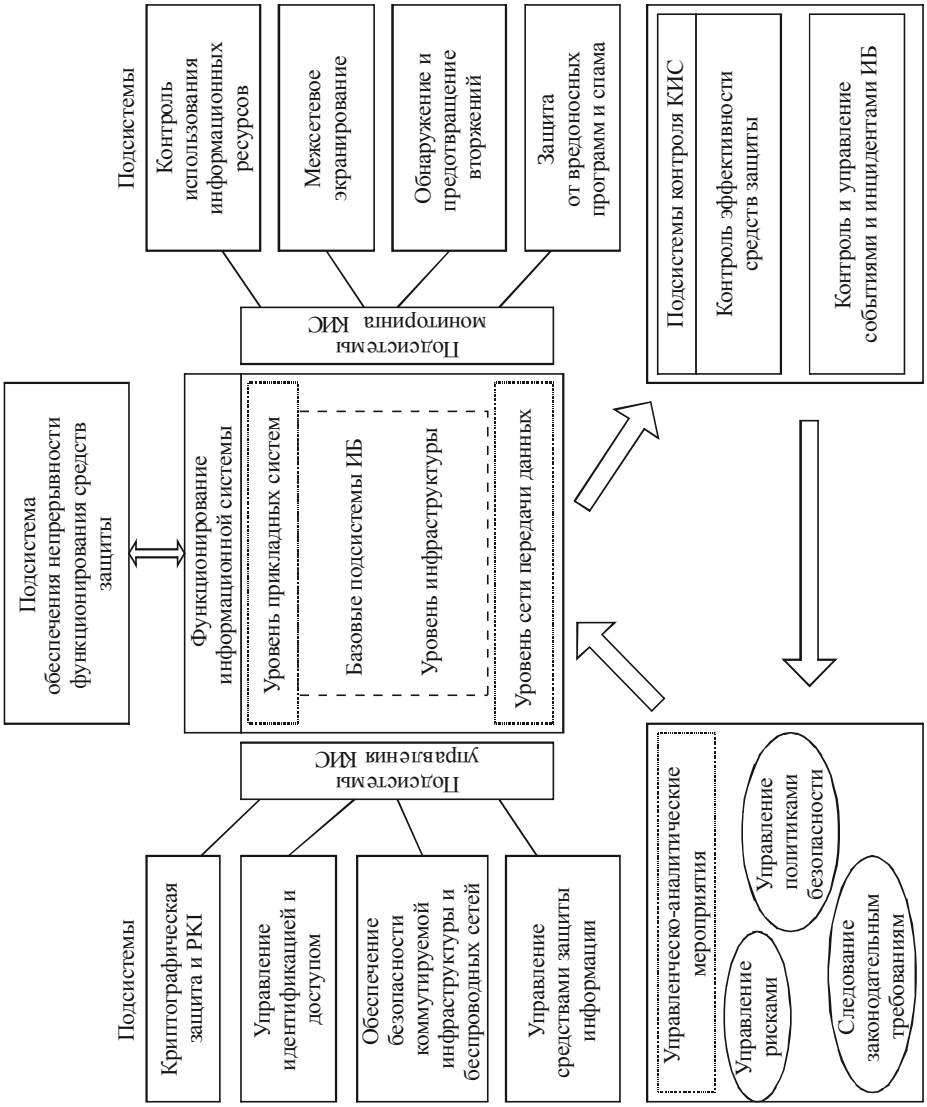

Рис.6.4. Общая структура комплексной системы защиты информации КИС

Приведем краткую характеристику подсистем информационной безопасности КИС. Наиболее важные технологии защиты корпоративной информации подробно рассмотрены в последующих главах.

6.4. Подсистемы информационной безопасности КИС

Подсистемы информационной безопасности являются основой, на которой строится вся защита информации КИС организации. Подсистемы безопасности позволяют обеспечить защиту информации на всех компонентах информационной системы организации и реализуются встроенными функциями обеспечения безопасности операционных систем (ОС), СУБД и прикладных систем, а также специализированными средствами защиты информации (СЗИ).

6.4.1. Подсистема защиты информации от несанкционированного доступа

Эта подсистема состоит из следующих трех подсистем:

- управления доступом;
- регистрации и учета;
- обеспечения целостности.

Система защиты от несанкционированного доступа должна обеспечивать четкую идентификацию *субъекта доступа*, *объекта доступа*, *типа доступа*.

Идентифицировав все параметры запроса, система производит проверку его легальности (санкционированности). Проверка легальности может проводиться как на основе *матрицы доступа*

(системы *дискреционного управления доступом*), так и на основе меток безопасности объекта и уровня допуска субъекта (*системы мандатного управления доступом*).

Существуют как узкоспециализированные системы защиты информации от несанкционированного доступа, так и решения, покрывающие все функции системы защиты информации [19].

Для того чтобы система защиты информации от НСД выполняла свои функции в полном объеме, необходима реализация дополнительных функциональных возможностей - регистрация и учет (аудит) событий в системе и обеспечение целостности защищаемой системы.

Функция регистрации и учета предназначена для фиксирования обращений к защищаемым ресурсам, что позволяет позже расследовать инциденты, связанные с утечкой или утратой информации ограниченного доступа. При этом необходимо учесть, что юридическую силу будет иметь только журнал сертифицированной системы.

Последняя важная задача защиты информации от НСД - это контроль и обеспечение целостности системы. В случае если программные или аппаратные компоненты системы подвергались модификациям, правильность выполнения основной функции системы может быть поставлена под сомнение. Поэтому необходимо, чтобы перед стартом компоненты системы сравнивались с эталоном, и при обнаружении расхождений пользователь оповещается о несанкционированной модификации системы и дальнейшая работа системы блокируется.

6.4.2. Подсистема криптографической защиты

Криптографическая защита данных обеспечивает безопасную передачу данных, а также их хранение. Криптографические методы защиты информации могут применяться на любом уровне взаимодействия информационных систем. Использование криптографических протоколов позволяет придать юридическую значимость процессам обработки электронных документов. Важным компонентом подсистемы криптографической защиты является инфраструктура управления открытыми ключами PKI (Public Key Infrastructure).

Инфраструктура управления открытыми ключами PKI предназначена для обеспечения защиты и организации безопасного обмена информацией в публичных (Интернет, Экстранет) и частных (Интранет) сетях за счет использования средств шифрования с открытыми ключами и механизма электронной цифровой подписи. Внедрение инфраструктуры открытых ключей на предприятии позволяет установить доверительные отношения между внутренними, а также внешними пользователями, обеспечить защиту приложений. Инфраструктура управления открытыми ключами и ее компоненты являются основой для создания комплексной системы обеспечения безопасности организации.

Широкое применение криптографических методов защиты информации делает подсистему криптографической защиты наиболее востребованной на рынке в настоящее время, однако данная подсистема не может в одиночку обеспечить комплексную защиту информации предприятия.

6.4.3. Подсистема управления идентификацией и доступом

С ростом числа пользователей информационной системы и числа прикладных систем и сервисов, к которым они должны получать доступ, увеличиваются затраты на администрирование учетных записей пользователей и управление правами доступа к системам и сервисам. Подсистема управления идентификацией и доступом предназначена для повышения безопасности корпоративных приложений и сервисов, а также для снижения затрат на администрирование пользователей в разнородных приложениях и операционных системах.

Подсистема управления идентификацией и доступом строится на основе:

- служб каталогов;
- систем централизованного управления учетными записями и правами доступа (Identity Management);
- средств однократной аутентификации (Single Sign-On);
- средств двухфакторной аутентификации.

При создании учетной записи пользователя в центральной системе (служба каталога, кадровая система и т.п.) подсистема управления идентификацией и доступом производит автоматическую трансформацию записи в идентификационные записи в целевых системах согласно политикам управления. Такой подход позволяет реализовать модель ролевого управления пользователями, которые автоматически получают необходимые им права на ресурсы в соответствии с должностными обязанностями, определенными через включение их в соответствующие ролевые группы. Альтернативой системе централизованного управления учетными записями и правами доступа выступают системы однократной аутентификации (Single Sign-On).

Использование подсистемы управления идентификацией и доступом позволяет автоматизировать процессы, связанные с созданием, администрированием, удалением учетных записей, предоставлением доступа к ресурсам и управлением правами в разнородных операционных системах, службах каталогов и приложениях.

6.4.4. Подсистема обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей

Подсистема обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей основывается на применении технологий контроля и защиты сетевого доступа NAC, 802.1x, VLAN.

Технология трансляции сетевых адресов NAC (Network Address Translation) позволяет контролировать и проверять на соответствие политике информационной безопасности любой компьютер, подключающийся к корпоративной сети, стационарный или мобильный компьютер, получающий доступ через локальную или через глобальную сеть, через проводное или беспроводное подключение, выделенное или коммутируемое соединение.

Проверка подлинности IEEE 802.1x представляет собой механизм контроля доступа на основе портов, который можно настроить на выполнение взаимной проверки подлинности между клиентами и сетью. После реализации такой настройки любое устройство, которому не удалось пройти проверку подлинности, не сможет участвовать ни в каком взаимодействии с выбранной сетью. Данная технология позволяет отказаться от применения статических ключей шифрования WEP (Wireless Equivalent Privacy).

Помимо генерации и распределения динамических ключей шифрования, стандартом IEEE 802.1x предусмотрены регулярное изменение сеансовых ключей и мониторинг сетевого доступа (с целью учета использования сетевых ресурсов). По данному стандарту управление доступом осуществляется на основе идентификаторов (user name) и паролей пользователей или их цифровых сертификатов. Средства IEEE 802.1x совместимы с существующими системами аутентификации.

6.4.5. Подсистема управления средствами защиты информации

Современные корпоративные информационные системы, как правило, имеют значительные географические размеры, насчитывают множество единиц техники и программного обеспечения. Кроме того, требования бизнеса к надежности и безопасности корпоративных информационных систем приводят к росту степени интеграции подсистем друг с другом и усложнению конфигураций отдельных систем.

Чтобы группа администраторов была способна справиться с задачей эффективного управления информационной системой, необходимо применять решения, которые позволяют:

- осуществлять централизованное управление всеми программными и техническими средствами;
- автоматически распространять обновления программного обеспечения, а также дополнительные программные средства на рабочие станции и серверы;
- создавать типовые конфигурации для быстрого развертывания на новых единицах техники;
- создать централизованную базу учетных записей для всех активных сетевых устройств, рабочих станций и серверов.

Регулярное обновление программных средств корпоративной информационной системы позволяет избежать угрозы эксплуатации злоумышленниками известных уязвимостей программного обеспечения.

Централизованное управление конфигурацией рабочих станций, серверов, активного сетевого оборудования позволяет существенно сократить затраты на обеспечение актуальной конфигурации оборудования информационной системы предприятия. Системы централизованного управления непосредственно зависят от систем централизованного управления учетными записями и правами доступа, а также систем администрирования доступа к сетевому оборудованию.

6.4.6. Подсистема контроля использования информационных ресурсов

Подсистема контроля использования информационных ресурсов предназначена для комплексного контроля электронных информационных потоков в организации. Подсистема разделяется на подсистему контроля циркуляции конфиденциальной информации и подсистемы контроля использования сотрудниками организации сервисов электронной почты и интернет-ресурсов.

Средства контроля использования интернет-ресурсов и электронной почты предназначены для проверки передаваемых и принимаемых данных на соответствие тем или иным условиям информационного обмена и выполнения соответствующих действий по итогам проверки для предотвращения утечки конфиденциальной информации организации.

Применение систем контроля использования информационных ресурсов необходимо для снижения таких рисков, как:

- воздействие вредоносного ПО (вирусов, «червей», «троянских» программ);
- компьютерные атаки и скрытое проникновение в корпоративную сеть;
- случайная или умышленно организованная утечка конфиденциальной информации;
- бесконтрольный доступ к Интернету, приводящий к снижению производительности труда в организации и снижению пропускной способности корпоративной сети и каналов связи;
- получение нежелательной корреспонденции (спам).

Системы контроля использования электронной почты предназначены для реализации корпоративной политики путем контроля и архивации электронных отправлений. Все сообщения электронной почты проверяются системой на соответствие положениям политики использования электронной почты, система реагирует на нарушения этой политики согласно заданным правилам.

Системы контроля циркуляции конфиденциальной информации являются мощным классом систем, который предназначен для контроля и управления конфиденциальной информацией на всем ее жизненном цикле и включает в себя функциональность систем контроля доступа использования интернет-ресурсов и электронной почты.

6.4.7. Подсистема межсетевого экранирования

Сеть передачи данных является неотъемлемой частью любой организации, представляя собой платформу для функционирования сервисов и приложений корпоративной информационной системы. В то же время она может являться источником ряда инцидентов информационной безопасности, связанных с нарушением конфиденциальности, целостности и доступности информации, хранящейся и обрабатываемой на сетевых информационных ресурсах. Данные инциденты информационной безопасности могут быть связаны как с действиями внутренних или внешних злоумышленников, так и с действиями вредоносного программного кода.

Подсистема межсетевого экранирования обеспечивает защиту корпоративной сети передачи данных от внешних сетевых атак, а также защиту критичных внутренних сегментов сети, например сегмента администрирования или серверного сегмента, от действий внутреннего злоумышленника.

Межсетевые экраны могут представлять собой программно-аппаратные комплексы, функционирующие под управлением специально разработанной операционной системы, а также могут являться программными решениями. Для защиты корпоративной сети от внешних угроз межсетевые экраны устанавливаются на границе сети и представляют собой первый рубеж защиты периметра корпоративной информационной системы.

Средства межсетевого экранирования в составе корпоративной информационной системы могут работать совместно с рядом подсистем обеспечения ИБ. Интеграция с подсистемами управления и мониторинга позволяет реализовать централизованный контроль функционирования межсетевых экранов и принимать своевременные меры по предотвращению и минимизации последствий инцидентов ИБ. Интеграция межсетевых экранов с подсистемами обнаружения и предотвращения вторжений дает возможность совместить функции безопасности в одном устройстве и организовать единый интерфейс управления.

6.4.8. Подсистема обнаружения и предотвращения вторжений

Обнаружение вторжений - это процесс мониторинга событий, происходящих в информационной системе, и их анализа на наличие признаков, указывающих на попытки вторжения: нарушения конфиденциальности, целостности, доступности информации или нарушения политики информационной безопасности. *Предотвращение вторжений* - процесс блокировки выявленных вторжений.

Эта подсистема обеспечивает:

- предотвращение вторжений системного уровня;
- предотвращение вторжений сетевого уровня;
- защиту от атак DDoS.

Атаки DDoS (Distributed Denial of Service - распределенный отказ в обслуживании) являются одним из наиболее опасных по последствиям классов компьютерных атак, направленных на нарушение доступности информационных ресурсов.

Средства подсистемы обнаружения и предотвращения вторжений автоматизируют данные процессы и необходимы в организации любого уровня, чтобы предотвратить ущерб и потери, к которым могут привести вторжения.

6.4.9. Подсистема защиты от вредоносных программ и спама

Подсистема защиты от вредоносных программ и нежелательной корреспонденции (спама) включает в себя:

- антивирусную защиту серверов и рабочих станций;
- антивирусную защиту сообщений электронной почты;
- потоковую антивирусную фильтрацию;
- защиту от нежелательной корреспонденции.

Средства антивирусной защиты должны обеспечивать защиту от вредоносных программ во всех возможных точках их проникновения:

- защиту серверов и рабочих станций пользователей и администраторов;

- защиту почтовых систем;
- защиту шлюзов входа/выхода во внешнюю сеть.

Использование средств антивирусной защиты позволяет предотвратить ущерб из-за уничтожения, искажения ценной информации или нарушения работы средств вычислительной техники.

Подсистема защиты от вредоносных программ интегрируется с подсистемами:

- обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей для обеспечения блокировки зараженных узлов;
- межсетевого экранирования с целью перенаправления потенциально опасного трафика для антивирусной проверки;
- обеспечения непрерывности функционирования средств защиты с целью резервного копирования конфигураций средств антивирусной защиты и антивирусных баз;
- мониторинга и управления инцидентами для оперативного анализа инцидентов вирусного заражения их обработки, оповещения ответственных лиц.

6.4.10. Подсистема контроля эффективности защиты информации

Данная подсистема позволяет автоматизировать процесс контроля эффективности защиты информации:

- анализ уязвимостей сетевой и системной инфраструктуры - деятельность по выявлению уязвимостей в программно-аппаратном обеспечении на основе всесторонних или выборочных тестов сетевых сервисов, операционных систем, прикладного программного обеспечения, маршрутизаторов, межсетевых экранов и т.п.;
- анализ уязвимостей СУБД или Web-приложений - используется для выявления уязвимостей, характерных исключительно для баз данных или Web-приложений и Web-сервисов;
- контроль политик безопасности - деятельность по контролю выполнения правил политики безопасности. Это позволяет в любой момент времени иметь актуальную информацию об элементах ИС, состояние которых нарушает политику безопасности, и оперативно устранять несоответствия.

Подсистема контроля эффективности защиты информации интегрируется с подсистемами:

- обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей для обеспечения блокировки уязвимых узлов и узлов, не соответствующих политике информационной безопасности;
- обнаружения и предотвращения вторжений для возможности выбора способа противодействия в зависимости от критичности атаки;
- мониторинга и управления инцидентами для управления информацией об актуальных рисках, оперативного анализа и обработки наиболее критических инцидентов;
- управления обновлениями для оперативного устранения уязвимостей, связанных с отсутствием своевременно установленных обновлений безопасности.

6.4.11. Подсистема мониторинга и управления инцидентами информационной безопасности

Под *событием информационной безопасности* понимается состояние системы, сервиса или сети, которое свидетельствует о возможном нарушении политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности. *Инцидент информационной безопасности* - это одно или серия событий безопасности, которые могут привести к ущербу и потерям для организации.

Процесс управления инцидентами информационной безопасности играет важную роль в обеспечении информационной безопасности предприятия. Основной целью данного процесса является обеспечение эффективного разрешения инцидентов информационной безопасности, минимизация потерь для организации, вызванных инцидентами, и уменьшение риска возникновения повторных инцидентов.

Типовые действия, выполняемые в рамках процесса управления инцидентами информационной безопасности, включают:

- идентификацию инцидента информационной безопасности;
- реагирование на инцидент информационной безопасности;
- восстановление после инцидента информационной безопасности;
- последующие действия по инциденту (анализ первопричин возникшего инцидента, проведение служебного расследования и др.).

Автоматическое реагирование на события безопасности в соответствии с заданными правилами обработки и корреляции позволяет ускорить реакцию на возникающие инциденты ИБ и обеспечить защищенность корпоративной сети и информационных систем в круглосуточном режиме.

Средства мониторинга и управления инцидентами информационной безопасности интегрируют в себя все системы и средства защиты организации.

6.4.12. Подсистема обеспечения непрерывности функционирования средств защиты

Подсистема обеспечения непрерывности функционирования средств защиты включает в себя:

- резервное копирование и восстановление;
- обеспечение бесперебойного электропитания.

Система резервного копирования является служебной подсистемой системы хранения данных и предназначена для создания резервных копий и восстановления данных. Она позволяет защитить данные от разрушения не только в случае сбоев или выхода из строя аппаратуры, но и в результате ошибок программных средств и пользователей.

От надежности и стабильности системы бесперебойного питания напрямую зависит функционирование средств и систем защиты организации. Средства обеспечения бесперебойного питания предназначены:

- для стабилизации напряжения питания, фильтрации помех и скачков напряжения;
- для обеспечения непрерывного электропитания при всех видах нарушений внешнего питания, в том числе и при полном его отключении.

Использование централизованной системы резервного копирования позволяет сократить совокупную стоимость владения системами и средствами защиты.

Вопросы для самоконтроля

1. Сформулируйте основополагающие принципы построения современных КИС.
2. Охарактеризуйте четыре уровня управления КИС.
3. Укажите необходимые условия обеспечения санкционированного доступа к информационным ресурсам предприятия.
4. Какие важные системные функции может выполнять КИС при реализации в ней принципа централизованного управления?
5. Объясните значение управления рисками предприятия для создания системы эффективной защиты информации на этом предприятии.
6. Какие требования необходимо учитывать при разработке архитектуры КСЗИ?
7. Перечислите меры и средства защиты, применяемые при построении комплексной системы защиты информации КИС.
8. Укажите основные подсистемы информационной безопасности, входящие в состав КСЗИ.
9. Опишите особенности подсистемы защиты информации от несанкционированного доступа.
10. Опишите назначение и особенности подсистемы контроля эффективности защиты информации.
11. Опишите назначение и особенности подсистемы мониторинга и управления инцидентами ИБ.
12. Опишите назначение и особенности подсистемы обеспечения непрерывности функционирования средств защиты.

Глава 7. Защита от вредоносных программ и спама

Безопасность - это предотвращение вреда.
Платон. «Диалоги»

Существуют программы, намеренно написанные с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов. Такие программы несут вредоносную нагрузку и соответственно называются вредоносными.

7.1. Классификация вредоносных программ

Вредоносные программы классифицируют по способу проникновения, размножения и типу вредоносной нагрузки.

В соответствии со способами распространения и вредоносной нагрузки все вредоносные программы можно разделить на четыре основных типа - компьютерные вирусы, «черви», «трояны» и другие программы.

Следует отметить, что термином «компьютерный вирус» часто называют любую вредоносную программу. Это обусловлено тем, что первые известные вредоносные программы были именно компьютерными вирусами и в течение последующих десятилетий число вирусов значительно превышало количество всех остальных вредоносных программ. Однако в последнее время наметились тенденции к появлению новых, невирусных технологий, которые используют вредоносные программы. При этом доля истинных вирусов в общем числе инцидентов с вредоносными программами за последние годы значительно сократилась.

В настоящее время вредоносные программы - это уже большей частью именно не вирусы, хотя такие термины как «вирусы» и «заражение вирусом» применяются по отношению ко всем вредоносным программам. Поэтому далее под термином «вирус» будет пониматься и вредоносная программа.

Компьютерные вирусы. Это программа, способная создавать свои дубликаты и внедрять их в компьютерные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Основная цель любого компьютерного вируса - это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя (например, 26 числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

Жизненный цикл любого компьютерного вируса можно разделить на четыре этапа:

- проникновение на чужой компьютер;
- активация;
- поиск объектов для заражения;
- подготовка и внедрение копий.

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения - фактически все каналы, по которым можно скопировать файл. Однако в отличие от «червей», вирусы не используют сетевые ресурсы - заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал. Например, скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

После проникновения следует активация вируса. Это может происходить разными путями. В зависимости от выбранного метода вирусы делятся на следующие виды:

- *загрузочные вирусы* - заражают загрузочные сектора жестких дисков и мобильных носителей;
- *файловые вирусы* - заражают файлы.

Дополнительным признаком отличия вирусов от других вредоносных программ служит их привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Например, вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например Unix.

При подготовке своих копий вирусы могут применять для маскировки разные технологии:

- *шифрование* - в этом случае вирус состоит из двух частей: сам вирус и шифратор;
- *метаморфизм* - при применении этого метода вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительного, обычно ничего не делающих команд.

Соответственно в зависимости от используемых методов маскировки вирусы можно делить на шифрованные, метаморфные и полиморфные, использующие комбинацию двух типов маскировки.

Сетевые «черви». В отличие от вирусов сетевые «черви» - это вполне самостоятельные вредоносные программы. Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов.

В зависимости от способа проникновения в систему «черви» делятся на следующие типы:

- *сетевые «черви»* - используют для распространения локальные сети и Интернет;
- *почтовые «черви»* - распространяются с помощью почтовых программ;
- *IM-«черви»* - используют программы обмена сообщениями IM (Instant Messenger) в режиме реального времени;
- *IRC-«черви»* - распространяются через чаты IRC (Internet Relay Chat);
- *P2P-«черви»* - распространяются при помощи пиринговых файлообменных сетей P2P (peer-to-peer - равный с равным).

После проникновения на компьютер «червь» должен активироваться, иными словами, запуститься. По методу активации все черви можно разделить на две большие группы - на тех, которые требуют активного участия пользователя, и тех, кто его не требует.

Отличительная особенность «червей» из первой группы - это использование обманных методов. Например, получатель инфицированного файла вводится в заблуждение текстом полученного письма и добровольно открывает вложение с почтовым червем, тем самым его активируя. «Черви» из второй группы используют ошибки в настройке или бреши в системе безопасности операционной системы. В последнее время наметилась тенденция к совмещению этих двух технологий - такие «черви» наиболее опасны и часто вызывают глобальные эпидемии.

Сетевые «черви» могут кооперироваться с вирусами - такая пара способна самостоятельно распространяться по сети (благодаря «червю») и в то же время заражать ресурсы компьютера (функции вируса).

«Троянские» программы. Программа класса «*троянский конь*» (или просто «*троян*») имеет только одно назначение - нанести ущерб целевому компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

В отличие от вирусов и «червей», «трояны» сами не размножаются. Жизненный цикл троянов состоит из трех этапов:

- проникновение в систему;
- активация;
- выполнение вредоносных действий.

Некоторые «трояны» способны к самостоятельному преодолению систем защиты компьютерной системы с целью проникновения в нее. В этом случае обычно применяется маскировка, когда «троян» выдает себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск (например, загружает из Интернет) и запускает. При этом программа действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные «трояну».

Однако в большинстве случаев «трояны» проникают на компьютеры вместе с вирусом либо «червем». Такие «трояны» можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу.

После проникновения на компьютер «трояну» необходима активация. И здесь он похож на «червя» - либо требует активных действий от пользователя или через уязвимости в программном обеспечении самостоятельно заражает систему.

Поскольку главная цель «троянов» - это выполнение несанкционированных действий, они классифицируются по типу вредоносной нагрузки:

- *похитители паролей* - предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат;
- *утилиты скрытого удаленного управления* - это «трояны», которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы. Такие «трояны» могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных;
- *логические бомбы* - характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например удаление файлов;
- *клавиатурные шпионы* - постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору;
- *анонимные SMTP-серверы и прокси-серверы* - такие «трояны» на зараженном компьютере организовывают несанкционированную отправку электронной почты, что часто используется для рассылки спама;
- *утилиты дозвона* в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернет;

- *модификаторы настроек браузера* - меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т.п.

Отдельно отметим, что существуют программы из класса «троянов», которые наносят вред другим, удаленным компьютерам и сетям, при этом не нарушая работоспособности инфицированного компьютера. Яркие представители этой группы - *организаторы атак DDoS*.

Другие вредоносные программы и нежелательная корреспонденция. Кроме вирусов, «червей» и «троянов», существует еще много других вредоносных программ и нежелательной корреспонденции. Среди них можно выделить следующие группы.

- *Шпионское ПО (spyware)* - опасные для пользователя программы, предназначенные для слежения за системой и отсылки собранной информации третьей стороне - создателю или заказчику такой программы. Среди заказчиков шпионского ПО - спамеры, рекламщики, маркетинговые агентства, преступные группировки, деятели промышленного шпионажа. Шпионские программы «интересуют» системные данные, тип браузера, посещаемые Web-узлы, иногда и содержимое файлов на жестком диске компьютера-жертвы. Такие программы тайно закачиваются на компьютер вместе с каким-нибудь бесплатным софтом или при просмотре определенным образом сконструированных HTML-страниц и всплывающих рекламных окон и самоустанавливаются без информирования об этом пользователя. Побочные эффекты от присутствия шпионского ПО на компьютере - нестабильная работа браузера и замедление производительности системы.
- *Условно опасные программы*, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:

- *аплеты (applets)* - прикладные программы, небольшие Java-приложения, встраиваемые в HTML-страницы. По своей сути эти программы не вредоносные, но могут использоваться в злонамеренных целях. Особенно аплеты опасны для любителей онлайновых игр, так как в них аплеты Java требуются обязательно. Аплеты, как и шпионское ПО, могут использоваться для отправки собранной на компьютере информации третьей стороне;
- *рекламные утилиты (adware)* - условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается и программы начинают работать в обычном режиме. Проблема adware кроется в механизмах, которые используются для загрузки рекламы на компьютер. Кроме того, для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже после регистрации такие модули могут автоматически не удаляться и продолжать свою работу в скрытом режиме;
- *riskware* - вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернет, утилиты восстановления забытых паролей и др.

- *Хакерские утилиты* - к этому виду программ относятся программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых «червей», компьютерных вирусов и «троянских» программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit) и другие подобные утилиты. Такие специфические программы обычно используют только хакеры.
- *Мистификации* - программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений, например, о форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений зависит от фантазии автора программы.
- *Спам* - нежелательная почтовая корреспонденция рекламного характера, загружающая трафик и отнимающая время у пользователей.

7.2. Основы работы антивирусных программ

Самыми эффективными средствами защиты от вирусов являются специальные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах. Такие программы называются антивирусами, и для того чтобы построить действительно надежную антивирусную защиту, использовать их нужно обязательно.

В современных антивирусных продуктах используются два основных подхода к обнаружению вредоносных программ: сигнатурный и проактивный/эвристический. *Сигнатурные методы* - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов. *Проактивные/эвристические методы* - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

7.2.1. Сигнатурный анализ

Термин «*сигнатура*» происходит от английского слова «*signature*», которое означает «подпись» или же в переносном смысле - «характерная черта, нечто идентифицирующее».

Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиске вирусов путем сравнения файлов с выявленными чертами.

Сигнатурой вируса будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле (включая случаи, когда файл целиком является вирусом). Все вместе сигнатуры известных вирусов составляют *антивирусную базу*.

Эта технология предполагает непрерывное отслеживание новых экземпляров вредителей, их описание и включение в базу сигнатур. Задачу выделения сигнатур, как правило, решают люди - эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска. В наиболее простых случаях могут применяться специальные автоматизированные средства выделения сигнатур. Например, в случае несложных по структуре «троянов» или «червей», которые не заражают другие программы, а целиком являются вредоносными программами.

Практически в каждой компании, выпускающей антивирусы, есть своя группа экспертов, выполняющая анализ новых вирусов и пополняющая антивирусную базу новыми сигнатурами. По этой причине антивирусные базы в разных антивирусах отличаются. Тем не менее, между антивирусными компаниями существует договоренность об обмене образцами вирусов, а значит рано или поздно сигнатура нового вируса попадает в антивирусные базы практически всех антивирусов. Лучшим же антивирусом будет тот, для которого сигнатура нового вируса была выпущена раньше всех.

Часто для обнаружения семейства похожих вирусов используется одна сигнатура, и поэтому количество сигнатур не всегда равно количеству обнаруживаемых вирусов. Соотношение количества сигнатур и количества известных вирусов для каждой антивирусной базы свое. Если же учесть, что антивирусные компании обмениваются образцами вирусов, можно с высокой долей уверенности считать, что антивирусные базы наиболее известных антивирусов эквивалентны.

Важное дополнительное свойство сигнатур - точное и гарантированное определение типа вируса. Это свойство позволяет занести в базу не только сами сигнатуры, но и способы лечения вируса.

Главные критерии эффективности сигнатурного метода - это скорость реакции на новые угрозы, частота обновлений, максимальное число обнаруженных угроз.

Главный недостаток сигнатурного метода - задержка при реакции на новые угрозы. Для получения сигнатуры необходимо иметь образец вируса. Создать его сигнатуру невозможно, пока вирус не попал на анализ к экспертам. Поэтому сигнатуры всегда появляются только через некоторое время после появления нового вируса. Именно поэтому сигнатурный метод непригоден для оперативной защиты от вновь появляющихся вирусов.

С момента появления вируса в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вирус способен заражать компьютеры почти беспрепятственно. Однако в защите от новых вирусов помогают используемые в антивирусных программах проактивные/эвристические методы обнаружения вирусов.

7.2.2. Проактивные методы обнаружения

Проактивные методы обнаружения вирусов получают все большее распространение. В принципе, использование этой технологии позволяет обнаруживать еще неизвестные вредоносные программы. Существует несколько подходов к проактивной защите.

Рассмотрим два наиболее популярных подхода: эвристические анализаторы и поведенческие блокираторы.

Эвристические анализаторы. Слово «*эвристика*» происходит от греческого глагола «находить». Суть *эвристических методов* состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок. Такое определение звучит достаточно сложно, поэтому эвристический метод поясним далее на примерах.

Если сигнатурный метод основан на выделении характерных признаков вируса и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на предположении (весьма правдоподобном), что новые вирусы часто оказываются похожи на какие-либо из уже известных. Такое предположение оправдывается наличием в антивирусных базах сигнатур для определения не одного, а сразу нескольких вирусов. Этот эвристический метод часто называют *поиском вирусов, похожих на известные*, или *статическим анализом*.

Эвристический анализатор (эвристик) - это программа, которая анализирует программный код проверяемого объекта и по косвенным признакам определяет, является ли объект вредоносным. Работа эвристического анализатора, как правило, начинается с поиска в программном коде подозрительных признаков (команд), характерных для вредоносных программ. Например, многие вредоносные коды ищут исполняемые программы, открывают найденные файлы и изменяют их. Эвристический анализатор просматривает код приложения и, встретив подозрительную команду,

увеличивает некий «счетчик подозрительности» для данного приложения. Если после просмотра всего кода значение счетчика превышает заданное пороговое значение, то объект признается подозрительным.

Первые эвристические анализаторы появились в антивирусных продуктах довольно давно, и на сегодняшний день более или менее совершенные эвристики реализованы во всех антивирусных решениях.

Достоинствами статического анализа являются простота реализации, высокая скорость работы, возможность обнаружения новых неизвестных вирусов еще до того, как для них будут выделены сигнатуры. Однако уровень обнаружения новых вредоносных кодов остается довольно низким, а вероятность ложных срабатываний высокой. Поэтому в современных антивирусах статический анализ используется в сочетании с динамическим. Идея такого комбинированного подхода состоит в том, чтобы до того как приложение будет запущено на компьютере пользователя, эмулировать его запуск в безопасном виртуальном окружении, которое называется также буфером эмуляции, или «песочницей».

Динамический эвристический анализатор читает часть кода приложения в буфер эмуляции антивируса и с помощью специальных приемов эмулирует его исполнение. Если в процессе этого «псевдоисполнения» обнаруживаются какие-либо подозрительные действия, объект признается вредоносным и его запуск на компьютере пользователя блокируется.

В отличие от статического метода, динамический более требователен к ресурсам ПК, так как для анализа приходится использовать безопасное виртуальное пространство, а запуск приложения на компьютере пользователя откладывается на время анализа. Однако и уровень обнаружения вредителей у динамического метода значительно выше статического, а вероятность ложных срабатываний существенно меньше.

Недостатки эвристических анализаторов:

- невозможность лечения - в силу возможных ложных срабатываний и возможного неточного определения типа вируса, попытка лечения может привести к большим потерям информации, чем сам вирус, а это недопустимо;
- низкая эффективность против принципиально новых типов вирусов.

Поведенческие блокираторы. Поведенческий блокиратор - это программа, которая анализирует поведение запущенного приложения и блокирует любые опасные действия. К основным вредоносным действиям относятся:

- удаление файла;
- запись в файл;
- запись в определенные области системного реестра;
- открытие порта на прослушивание;
- перехват данных, вводимых с клавиатуры;
- рассылка писем и др.

Выполнение каждого такого действия по отдельности не является поводом считать программу вредоносной. Но если программа последовательно выполняет несколько таких действий, например перехватывает данные, вводимые с клавиатуры, и с определенной частотой пересылает эти данные на какой-то адрес в Интернет, значит эта программа, по меньшей мере, подозрительна.

В отличие от эвристических анализаторов, где подозрительные действия отслеживаются в режиме эмуляции (динамический эвристик), поведенческие блокираторы работают в реальных условиях.

Принцип действия первых поведенческих блокираторов был прост. При обнаружении потенциально опасного действия задавался вопрос пользователю: разрешить или запретить это действие. Во многих случаях такой подход работал, но «подозрительные» действия производили и легитимные программы (вплоть до операционной системы). Поэтому если пользователь не обладал должной квалификацией, вопросы антивируса вызывали непонимание.

Современные поведенческие блокираторы анализируют уже не отдельные действия, а последовательность операций. Другими словами, заключение об опасности того или иного приложения выносится на основе более сложного анализа. Таким образом, удается значительно сократить количество запросов к пользователю и повысить надежность детектирования.

Современные поведенческие блокираторы способны контролировать широкий спектр событий, происходящих в системе. Это прежде всего контроль опасной активности (анализ поведения всех процессов, запущенных в системе, сохранение всех изменений, производимых в файловой системе и реестре).

При выполнении некоторым приложением набора подозрительных действий выдается предупреждение пользователю об опасности данного процесса. Помимо этого блокиратор позволяет перехватить все возможности внедрения программного кода в чужие процессы. Вдобавок блокиратор способен обнаружить *руткиты*, т.е. программы, которые скрывают от пользователя работу вредоносного кода с файлами, папками и ключами реестра, а также прячут запущенные программы, системные службы, драйверы и сетевые соединения.

Особо стоит выделить такую функциональность поведенческих блокираторов, как контроль целостности приложений и системного реестра Microsoft Windows. В последнем случае блокиратор контролирует изменения ключей реестра и позволяет задавать правила доступа к ним для различных приложений. Все вместе это позволяет осуществить откат изменений после определения опасной

активности в системе. Таким образом, можно восстанавливать систему даже после вредоносных действий неизвестных программ, вернув ее к незараженному состоянию.

В качестве примера эффективного поведенческого блокиратора нового поколения можно привести модуль проактивной защиты (Proactive Defence Module), реализованный в продуктах «Лаборатории Касперского». Данный модуль включает в себя все перечисленные выше возможности и, что особенно важно, хорошую систему информирования пользователя о том, в чем реально состоит опасность тех или иных подозрительных действий. Любой поведенческий блокиратор на определенном этапе требует вмешательства пользователя, что предполагает наличие у последнего определенной квалификации. На практике пользователь часто не обладает необходимыми знаниями, поэтому информационная поддержка - фактически поддержка принятия решений - является обязательным атрибутом современных антивирусных решений.

Поведенческий блокиратор может предотвратить распространение как известного, так и неизвестного (написанного после создания блокиратора) вируса, что является неоспоримым достоинством такого подхода к защите.

Недостатком поведенческих блокираторов остается срабатывание на действия ряда легитимных программ. Для принятия окончательного решения о вредоносности приложения требуется вмешательство пользователя, что предполагает наличие у него достаточной квалификации.

Проактивный подход к борьбе с вредоносными программами стал ответом разработчиков антивирусов на все возрастающий поток новых вредителей и увеличивающуюся скорость их распространения. Существующие сегодня проактивные методы действительно позволяют бороться со многими новыми угрозами. Однако проактивные технологии не позволяют полностью отказаться от обновлений антивирусной защиты. Проактивные методы, так же как и сигнатурные, требуют регулярных обновлений.

Для оптимальной антивирусной защиты необходимо сочетание проактивных и сигнатурных подходов. Максимального уровня обнаружения угроз можно достигнуть только комбинируя эти методы. Примером успешного сочетания проактивных и сигнатурных методов может служить технология ThreatSense компании Eset.

ThreatSense - это сбалансированная технология, позволяющая комбинировать эвристический анализатор и поведенческий блокиратор с сигнатурным методом. Эта технология обеспечивает обнаружение не только известных, но и новых угроз, не снижая при этом скорости работы используемой системы.

Практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.

7.2.3. Дополнительные модули

Практически любой антивирус сегодня использует все известные методы обнаружения вирусов. Но одних средств обнаружения мало для успешной работы антивируса. Для того чтобы чисто антивирусные средства были эффективными, нужны дополнительные модули, выполняющие вспомогательные функции.

Модуль обновления. Каждый антивирус должен содержать модуль обновления. Это связано с тем, что основным методом обнаружения вирусов сегодня является сигнатурный анализ, который полагается на использование антивирусной базы.

Чтобы сигнатурный анализ эффективно справлялся с самыми последними вирусами, антивирусные эксперты постоянно анализируют образцы новых вирусов и выпускают для них сигнатуры. После этого главной проблемой становится доставка сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу. Именно эту задачу и решает модуль обновления.

После того как эксперты создали новые сигнатуры, файлы с сигнатурами размещаются на серверах компании - производителя антивируса и становятся доступными для загрузки. Модуль обновления обращается к этим серверам, определяет наличие новых файлов, загружает их на компьютер пользователя и дает команду антивирусным модулям использовать новые файлы сигнатур.

Модуль планирования. Модуль планирования является вторым важным вспомогательным модулем. Существует ряд действий, которые антивирус должен выполнять регулярно: проверять весь компьютер на наличие вирусов и обновлять антивирусную базу.

В настоящее время новые модификации вредоносных программ обнаруживаются постоянно, что вынуждает антивирусные компании выпускать новые файлы сигнатур для обновления антивирусной базы буквально каждый час. Разумным расписанием для проверки компьютера можно считать раз в неделю. Модуль планирования позволяет настроить периодичность выполнения этих действий.

Модуль управления. По мере увеличения количества модулей в антивирусе возникает необходимость в дополнительном модуле для управления и настройки. Основные требования к такому модулю - удобный доступ к настройкам, интуитивная понятность, подробная справочная система, описывающая каждую настройку, возможность защитить настройки от изменений, если за компьютером работает несколько человек. Подобным модулем управления обладают антивирусы для домашнего использования.

Антивирусы для защиты компьютеров в крупных сетях должны обладать несколько иными свойствами. Такие антивирусы оборудованы специальным модулем управления. Основные свойства этого модуля управления:

- *поддержка удаленного управления и настройки* - администратор безопасности может запускать и останавливать антивирусные модули, а также менять их настройки по сети, не вставая со своего места;
- *защита настроек от изменений* - модуль управления не позволяет локальному пользователю изменять настройки или останавливать антивирус, чтобы пользователь не мог ослабить антивирусную защиту организации.

Карантин. Во многих антивирусах среди вспомогательных средств имеется специальная технология - *карантин*, которая защищает от возможной потери данных в результате действий антивируса. Например, нетрудно представить ситуацию, при которой файл детектируется как возможно зараженный эвристическим анализатором и удаляется согласно настройкам антивируса.

Однако эвристический анализатор никогда не дает стопроцентной гарантии того, что файл действительно заражен, а значит с определенной вероятностью антивирус мог удалить незараженный файл. Или же антивирус обнаруживает важный документ, зараженный вирусом, и пытается согласно настройкам выполнить лечение, но по каким-то причинам происходит сбой и вместе с вылеченным вирусом теряется важная информация. От таких случаев желательно застраховаться. Это можно сделать, если перед лечением или удалением файлов сохранить их резервные копии, тогда, если окажется, что файл был удален ошибочно или была потеряна важная информация, всегда можно будет выполнить восстановление из резервной копии.

7.2.4. Режимы работы антивирусов

Надежность антивирусной защиты обеспечивается не только способностью отражать любые вирусные атаки. Другое не менее важное свойство защиты - ее непрерывность. Это означает, что антивирус должен начинать работу по возможности до того, как вирусы смогут заразить только что включенный компьютер, и выключаться только после завершения работы всех программ.

Однако пользователь должен иметь возможность в любой момент запросить максимум ресурсов компьютера для решения своей прикладной задачи и антивирусная защита не должна ему мешать это сделать. Оптимальный выход в этой ситуации - это введение двух различных режимов работы антивирусных средств:

- непрерывная проверка на наличие вирусов с небольшой функциональностью в режиме реального времени;
- тщательная проверка на наличие вирусов по запросу пользователя.

Проверка в режиме реального времени. Проверка в режиме реального времени обеспечивает непрерывность работы антивирусной защиты. Это реализуется с помощью обязательной проверки всех действий, совершаемых другими программами и самим пользователем, на предмет вредоносности, вне зависимости от их исходного расположения - будь это свой жесткий диск, внешние носители информации, другие сетевые ресурсы или собственная оперативная память. Также проверке подвергаются все косвенные действия через третьи программы. Режим постоянной проверки защиты системы от заражения должен быть включен с момента начала загрузки операционной системы и выключаться только в последнюю очередь.

Проверка по требованию. В некоторых случаях наличия постоянно работающей проверки в режиме реального времени может быть недостаточно. Например, на компьютер был скопирован зараженный файл, исключенный из постоянной проверки ввиду больших размеров и, следовательно, вирус в нем обнаружен не был. Если этот файл на рассматриваемом компьютере запускаться не будет, то вирус может проявить себя только после пересылки его на другой компьютер, что может сильно повредить репутации отправителя - распространителя вирусов. Для исключения подобных случаев используется второй режим работы антивируса - проверка по требованию.

Для такого режима пользователь обычно сам указывает, какие файлы, каталоги или области диска необходимо проверить, а также время, когда нужно произвести такую проверку - в виде расписания или разового запуска вручную. Рекомендуется проверять все чужие внешние носители информации, такие, как дискеты, компакт-диски, flash-накопители, каждый раз перед чтением информации с них, а также весь свой жесткий диск не реже одного раза в неделю.

Тестирование работы антивируса. После того как антивирус установлен и настроен, необходимо убедиться, что все сделано правильно и антивирусная защита работает. Как проверить работу антивируса?

Использовать для тестирования настоящие вирусы крайне опасно. Если пользователь неправильно выполнил установку или настройку антивируса, то в процессе такого тестирования он может заразить свой компьютер, в результате чего потерять данные или стать источником заражения для других компьютеров.

Нужен такой способ тестирования антивирусов, который был бы безопасным, но давал четкий ответ на вопрос, корректно ли работает антивирус.

Учитывая важность проблемы, организация EICAR при участии антивирусных компаний создала специальный тестовый файл, названный по имени организации - eicar.com.

Eicar.com - это исполняемый файл в COM-формате, который не выполняет никаких вредоносных действий, а просто выводит на экран строку «EICAR-STANDARD-ANTIVIRUS-TEST-FILE!». Получить eicar.com можно на сайте организации EICAR по адресу http://www.eicar.org/anti_virus_test_file.htm, но можно создать этот файл самостоятельно, используя редактор Notepad системы Windows.

Файл eicar.com позволяет протестировать, как антивирус справляется с файловыми вирусами и близкими по структуре вредоносными программами - большинством «троянов», некоторыми «червями».

7.2.5. Антивирусные комплексы

Второй способ оптимизации работы антивируса - это создание различных его версий для компьютеров, служащих разным целям. Зачастую они отличаются лишь наличием тех или иных специфических модулей и различием в интерфейсе, в то время как непосредственно антивирусная проверка осуществляется одной и той же подпрограммой, называемой антивирусным ядром.

Антивирусный комплекс - набор антивирусов, использующих одинаковое антивирусное ядро, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем. В антивирусный комплекс также в обязательном порядке входят средства обновления антивирусных баз.

Всякая локальная сеть, как правило, содержит компьютеры двух типов - рабочие станции, за которыми непосредственно сидят люди, и сетевые серверы, используемые для служебных целей. В соответствии с характером выполняемых функций серверы делятся на:

- *сетевые*, которые обеспечивают централизованное хранилище информации: файловые серверы, серверы приложений и др.;
- *почтовые*, на которых работает программа, служащая для передачи электронных сообщений от одного компьютера к другому;
- *шлюзы*, отвечающие за передачу информации из одной сети в другую. Например, шлюз необходим для соединения локальной сети с Интернет.

Соответственно различают четыре вида антивирусных комплексов - для защиты рабочих станций, файловых серверов, почтовых систем и шлюзов.

Рабочие станции - это компьютеры локальной сети, за которыми непосредственно работают пользователи. Главной задачей комплекса для защиты рабочих станций является обеспечение безопасной работы на рассматриваемом компьютере - для этого необходима проверка в режиме реального времени, проверка по требованию и проверка локальной электронной почты.

Сетевые серверы - это компьютеры, специально выделенные для хранения или обработки информации. Они обычно не используются для непосредственной работы за ними и поэтому в отличие от рабочих станций проверка электронной почты на наличие вирусов тут не нужна. Следовательно, антивирусный комплекс для файловых серверов должен проводить проверку в режиме реального времени и проверку по требованию.

Антивирусный комплекс для защиты *почтовых систем* предназначен для проверки всех проходящих электронных писем на наличие в них вирусов, т.е. проверять другие файлы, размещенные на этом компьютере, он не обязан (для этого существует комплекс для защиты сетевых серверов). Поэтому к нему предъявляются требования по наличию собственно программы для проверки всей принимаемой и отправляемой почтовой корреспонденции в режиме реального времени и дополнительно механизма проверки по требованию почтовых баз данных.

Аналогично в соответствии со своим назначением антивирусный комплекс для *шлюза* осуществляет только проверку проходящих через шлюз данных.

Поскольку все вышеперечисленные комплексы используют сигнатурный анализ, то в обязательном порядке в них должно входить средство для поддержания антивирусных баз в актуальном состоянии, т.е. механизм их обновления. Дополнительно часто оказывается полезным модуль для удаленного централизованного управления, который позволяет системному администратору со своего рабочего места настраивать параметры работы антивируса, запускать проверку по требованию и обновление антивирусных баз.

7.2.6. Дополнительные средства защиты

Возможности антивирусных программ расширяют дополнительные средства защиты от вредоносных программ и нежелательной корреспонденции. Такими средствами защиты являются:

- обновления, устраняющие уязвимости в операционной системе, через которые могут проникать вирусы;
- брандмауэры - программы, защищающие от атак по сети;
- средства борьбы со спамом.

Обновления ПО. Как известно, вирусы нередко проникают на компьютеры через уязвимости («дыры») в операционной системе или установленных программах. Причем чаще всего вредоносными программами используются уязвимости операционной системы Microsoft Windows, пакета приложений Microsoft Office, браузера Internet Explorer и почтовой программы Outlook Express.

Чтобы не дать вирусам возможности использовать уязвимость, операционную систему и программное обеспечение нужно обновлять. Производители, как правило, раньше вирусописателей узнают о «дырах» в своих программах и заблаговременно выпускают для них исправления.

Для загрузки и установки обновлений в большинстве программ и систем есть встроенные средства. Например, в Windows XP и Windows Vista имеется специальный компонент «Автоматическое обновление», параметры работы которого настраиваются в окне «Свойства системы».

В последнее время вредоносные программы, использующие уязвимости в Windows и прикладных программах, появляются вскоре после выхода исправлений к этим уязвимостям. В некоторых случаях вредоносные программы появляются даже раньше исправлений. Поэтому необходимо своевременно устанавливать исправления, используя для этого средства автоматической установки.

Брандмауэры. Для того чтобы удаленно воспользоваться уязвимостью в программном обеспечении или операционной системе, нужно установить соединение и передать специально сформированный пакет данных. От таких попыток проникновения и заражения можно защититься путем запрета определенных соединений. Задачу контроля соединений успешно решают программы-брандмауэры.

Брандмауэр - это программа, которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил. Правило брандмауэра задается несколькими атрибутами:

- *приложение* - определяет программу, к которой относится правило, так что одни и те же действия могут быть разрешены одним программам и запрещены другим. Например, получать и отправлять почту разумно разрешить только программе - почтовому клиенту;
- *протокол* - определяет протокол, используемый для передачи данных. Обычно можно выбрать между двумя протоколами TCP и UDP;
- *адреса* - определяет, для соединений с каких адресов или на какие адреса будет действовать правило;
- *порт* - задает номера портов, на которые распространяется правило;
- *направление* - позволяет отдельно контролировать входящие и исходящие соединения;
- *действие* - определяет реакцию на обнаружение соединения, соответствующего остальным параметрам. Реакция может быть - разрешить, запретить или спросить у пользователя.

Не обязательно задавать конкретные значения всем атрибутам правила. Можно создать правило, которое будет запрещать входящие соединения на TCP порт 111 для всех приложений или разрешать любые исходящие соединения для программы Internet Explorer.

Для борьбы с вирусами брандмауэры могут применяться следующим образом. Во-первых, брандмауэр можно успешно использовать для защиты от вредоносных программ, которые распространяются непосредственно по сети, используя уязвимости в операционной системе. Например, «червь» Sasser атакует службу Windows LSASS через TCP порт 445. Для защиты от «червя» достаточно создать в брандмауэре правило, запрещающее входящие соединения на этот порт. Брандмауэр можно использовать и для защиты от атак неизвестных вирусов. Во-вторых, брандмауэры можно применять для контроля исходящих соединений. Многие «троянские» программы, да и «черви», после выполнения вредоносной функции стремятся подать сигнал автору вируса. Например, «троянская» программа, ворующая пароли, будет пытаться переслать все найденные пароли на определенный сайт или почтовый адрес. Для того чтобы воспрепятствовать этому, можно настроить брандмауэр на блокирование всех неизвестных соединений: разрешить только соединения от доверенных программ, таких, как используемый браузер, почтовый клиент, программа мгновенного обмена сообщений, а все остальные соединения запретить.

Некоторые вредоносные программы пассивно ожидают соединения на каком-то из портов. Если входящие соединения разрешены, то автор вредоносной программы сможет через некоторое время обратиться на этот порт и забрать нужную ему информацию или же передать вредоносной программе новые команды. Чтобы этого не произошло, брандмауэр должен быть настроен на запрет входящих соединений на все порты, кроме фиксированного перечня портов, используемых известными программами или операционной системой.

В последнее время широко распространены универсальные защитные программы, объединяющие возможности брандмауэра и антивируса. Например, Kaspersky Internet Security, Norton Internet Security, McAfee Internet Security и пр.

7.3. Средства защиты от нежелательной корреспонденции

Для решения проблемы защиты от спама (нежелательной корреспонденции рекламного характера) используются специальные антиспамовые фильтры. Для фильтрации нежелательной почты в антиспамовых фильтрах применяется несколько методов.

- *Черные и белые списки адресов. Черный список* - это список тех адресов, письма с которых фильтр отбраковывает сразу, не применяя других методов. В этот список нужно заносить адреса, если с них постоянно приходят ненужные или, хуже того, зараженные письма. *Белый список* - это список адресов хорошо известных пользователю людей или организаций, которые передают только полезную информацию. Антиспамовый фильтр можно настроить так, что будут приниматься только письма от адресатов из белого списка.
- *Базы данных образцов спама*. Как и антивирус, антиспамовый фильтр может использовать базу данных образцов нежелательных писем для удаления писем, соответствующих этим образцам.

- *Анализ служебных заголовков*. В письме в относительно скрытой форме хранится служебная информация о том, с какого сервера было доставлено письмо, какой адресат является реальным отправителем и др. Используя эту информацию, антиспамовый фильтр может решать, является письмо спамом или нет. Например, некоторые почтовые серверы, часто использующиеся для рассылки спама, заносятся в специальные общедоступные черные списки, и если письмо было доставлено с такого сервера, вполне вероятно, что это спам. Другой вариант проверки - запросить у почтового сервера, действительно ли существует адресат, указанный в письме как отправитель. Если такого адресата не существует, значит письмо скорее всего является нежелательным.
- *Самообучение*. Антиспамовые фильтры можно «обучать», указывая вручную, какие письма являются нормальными, а какие нежелательными. Через некоторое время антиспамовый фильтр начинает с большой достоверностью самостоятельно определять нежелательные письма по их похожести на предыдущий спам и непохожести на предыдущие нормальные письма.

Использование антиспамовых фильтров помогает защититься и от некоторых почтовых «червей». Самое очевидное применение - это при получении первого зараженного письма (в отсутствие антивируса это можно определить по косвенным признакам) отметить его как нежелательное и в дальнейшем все другие зараженные письма будут заблокированы фильтром.

Более того, почтовые «черви» известны тем, что имеют большое количество модификаций, незначительно отличающихся друг от друга. Поэтому антиспамовый фильтр может помочь и в борьбе с новыми модификациями известных вирусов с самого начала эпидемии. В этом смысле антиспамовый фильтр даже эффективнее антивируса, так как необходимо дождаться обновления антивирусных баз, чтобы антивирус смог обнаружить новую модификацию.

7.4. Защита корпоративной сети от воздействия вредоносных программ и вирусов

В настоящее время одним из основных вопросов обеспечения безопасности корпоративной информации является защита от вредоносных программ. Защита от вредоносных программ не ограничивается лишь традиционной установкой антивирусных средств на рабочие станции пользователей. Это сложная задача, требующая комплексного подхода к решению [17, 23].

7.4.1. Подсистема защиты корпоративной информации от вредоносных программ и вирусов

Одно из главных преимуществ данного решения - рассмотрение подсистемы защиты корпоративной информации от вредоносных программ и вирусов как многоуровневой системы (рис.7.1) [23].

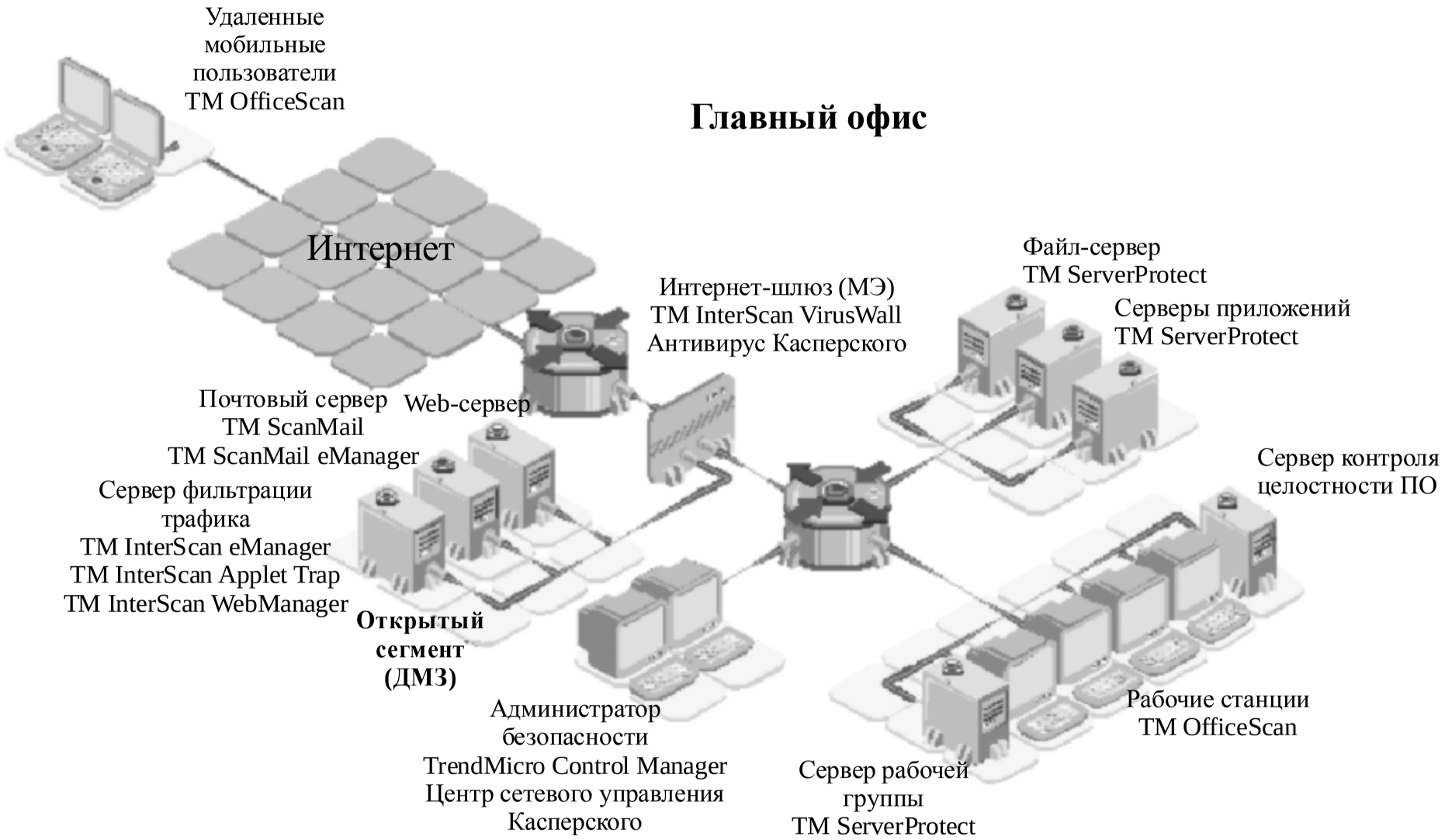

Рис.7.1. Схема защиты корпоративной сети от воздействия вредоносных программ и вирусов

Первый уровень включает в себя средства защиты от вредоносных программ, устанавливаемые на стыке с глобальными сетями (Интернет-шлюз и/или межсетевой экран, публичные серверы (Web, SMTP, ftp), размещаемые в демилитаризованной зоне) и осуществляющие фильтрацию основных видов трафика (HTTP, SMTP, FTP и т.д.). Антивирусные средства, устанавливаемые на МЭ, совместимы с Check Point FireWall-1 и Cisco PIX, которые являются одними из самых распространенных межсетевых экранов в России.

Второй уровень - средства защиты, устанавливаемые на внутренних корпоративных серверах и серверах рабочих групп (файловых хранилищах, серверах приложений и т.д.).

И, наконец, третий уровень - средства защиты от вредоносных программ, устанавливаемые на рабочих станциях пользователей, включая удаленных и мобильных пользователей.

В качестве средств защиты всех уровней выбраны продукты компании Trend Micro, а на шлюзе в дополнение к продуктам Trend Micro устанавливается Антивирус Касперского, повышая тем самым вероятность обнаружения вредоносных программ в точке их наиболее вероятного появления.

Преимущества данного решения заключаются в:

- использовании продуктов мировых лидеров;
- централизованном управлении всей подсистемой защиты от вредоносных программ;
- автоматическом обновлении антивирусных баз;
- тесном взаимодействии антивирусных средств всех уровней подсистемы и т.д.

Все эти преимущества обеспечивают высокую вероятность обнаружения вредоносных программ.

7.4.2. Серия продуктов Kaspersky Open Space Security для защиты корпоративных сетей от современных интернет-угроз

Серия продуктов *Kaspersky Open Space Security*, разработанная в Лаборатории Касперского, включает решения для защиты малых и крупных корпоративных сетей от всех видов современных интернет-угроз [17]. В серии продуктов Kaspersky Open Space Security реализована концепция защиты корпоративной сети, при которой безопасное рабочее пространство больше не ограничено стенами офиса, теперь оно охватывает и удаленных пользователей и сотрудников в командировке.

Основные возможности серии продуктов Kaspersky Open Space Security заключаются в следующем.

Kaspersky Open Space Security отвечает современным требованиям к системам защиты корпоративных сетей:

- решения для защиты каждого узла сети;
- технологии защиты от всех типов интернет-угроз;
- поддержка всех распространенных ОС / платформ;
- высокая скорость реакции на новые угрозы;
- комплексное применение различных технологий защиты.

Kaspersky Open Space Security позволяет использовать преимущества новых мобильных технологий, обеспечивая:

- полноценную защиту пользователей за пределами сети;
- комплексную безопасность пользователей смартфонов.

Kaspersky Open Space Security использует новые технологии защиты:

- защита от утечек информации;
- защита от руткитов;
- отмена вредоносных изменений;
- самозащита антивируса;
- защита данных при потере смартфона.

Kaspersky Open Space Security обеспечивает высокий уровень защиты сложных, распределенных сетей:

- централизованное администрирование;
- удаленная установка, управление и лечение;
- поддержка современных технологий Microsoft, Intel, Cisco;
- эффективное использование сетевых ресурсов.

В серию Kaspersky Open Space Security входят четыре продукта.

Kaspersky Work Space Security - защита рабочих станций (1-уровневая защита). Это решение для централизованной защиты рабочих станций, в том числе ноутбуков, и смартфонов в корпоративной сети и за ее пределами от всех видов современных интернет-угроз: вирусов, шпионских программ, хакерских атак и спама.

Kaspersky Business Space Security - защита рабочих станций и файловых серверов (2-уровневая защита). Это эффективная защита информационных ресурсов компании от современных интернет-угроз. Продукт Kaspersky Business Space Security защищает рабочие станции, смартфоны и файловые серверы от всех видов вирусов, «троянских» программ и «червей», предотвращает вирусные эпидемии, а также обеспечивает сохранность информации и мгновенный доступ пользователей к сетевым ресурсам. Продукт разработан с учетом повышенных требований к серверам, работающим в условиях высоких нагрузок.

Kaspersky Enterprise Space Security - защита рабочих станций, смартфонов, файловых и почтовых серверов (3-уровневая защита). Это решение обеспечивает свободный обмен информацией внутри компании и безопасные коммуникации с внешним миром. Продукт Kaspersky Enterprise Space Security защищает рабочие станции, смартфоны, а также файловые и почтовые серверы от всех видов современных интернет-угроз, удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и мгновенный безопасный доступ пользователей к сетевым ресурсам.

Kaspersky Total Space Security - защита рабочих станций, файловых и почтовых серверов, интернет-шлюзов (многоуровневая защита). Это решение защищает все узлы корпоративной сети любого масштаба и сложности от современных интернет-угроз. Решение Kaspersky Total Space Security контролирует все входящие и исходящие потоки данных: электронную почту, интернет-трафик и все сетевые взаимодействия. Продукт обеспечивает мгновенный и безопасный доступ пользователей к информационным ресурсам компании и сети Интернет, а также гарантирует безопасные коммуникации по электронной почте.

Вопросы для самоконтроля

1. Что такое вредоносная программа? Охарактеризуйте основные типы вредоносных программ.
2. Укажите существенные отличия компьютерных вирусов от сетевых «червей». Опишите основные особенности «троянских» программ.
3. Опишите два основных подхода к обнаружению вредоносных программ.
4. Как выполняется сигнатурный анализ? Каковы его достоинства и недостатки?
5. Что представляют собой проактивные методы обнаружения?
6. Опишите принцип действия, достоинства и недостатки эвристических анализаторов.
7. Опишите принцип действия, достоинства и недостатки поведенческих блокираторов.
8. Назовите и опишите дополнительные модули антивирусных средств.
9. Каковы дополнительные меры и средства защиты от вредоносных программ, расширяющие возможности антивирусных программ?
10. Опишите меры и средства защиты от спама (нежелательной корреспонденции).
11. Каковы особенности реализации подсистемы защиты корпоративной информации от вредоносных программ и вирусов?
12. Каковы возможности серии продуктов Kaspersky Open Space Security для защиты корпоративных сетей от современных интернет-угроз?

Глава 8. Обнаружение и предотвращение вторжений

Ищите и обрящете.
Евангелие от Матфея

Системы предотвращения вторжений IPS (Intrusion Prevention System) предназначены обеспечить безопасность защищаемых объектов от воздействия, которое признано вторжением в КИС.

Раньше на периметре сети устанавливали всего два класса защитных средств - межсетевые экраны (firewall) и системы обнаружения вторжений IDS (Intrusion Detection System). Межсетевые экраны пропускали трафик через себя, но не «заглядывали» внутрь пересылаемых данных, анализируя только заголовки IP-пакетов. Системы IDS, напротив, анализировали то, что упускалось из виду межсетевыми экранами, но не были способны блокировать атаки, так как трафик через них не проходил. На стыке этих двух технологий родился новый класс защитных средств - системы предотвращения вторжений IPS (Intrusion Prevention System).

Системы IPS оказались настолько популярными, что некоторые производители стали рекламировать свои IDS как системы предотвращения атак, т.е. IPS, тем самым незаслуженно открывая для себя новые рынки и новых клиентов.

На самом деле, системы предотвращения вторжений IPS существенно превосходят по своим возможностям системы обнаружения вторжений IDS. Системы IPS объединяют ряд технологий безопасности и достаточно далеко продвинулись по сравнению со своими предшественниками - системами обнаружения вторжений IDS.

8.1. Основные понятия

Обнаружение вторжений - это процесс мониторинга событий, происходящих в информационной системе, и их анализа на наличие признаков, указывающих на попытки вторжения: нарушения конфиденциальности, целостности, доступности информации или нарушения политики информационной безопасности.

Предотвращение вторжений - процесс блокировки выявленных вторжений.

Средства системы обнаружения и предотвращения вторжений IPS автоматизируют данные процессы и необходимы в организации любого уровня, чтобы предотвратить ущерб и потери, к которым могут привести вторжения.

В отличие от системы IDS, признаками настоящей системы IPS являются следующие:

- система IPS функционирует в режиме inline (пропускает трафик через себя) на скорости канала. Иначе говоря, решение IPS не снижает скорость передачи данных;
- система IPS обеспечивает сборку передаваемых пакетов в правильном порядке и анализирует эти пакеты с целью обнаружения следов несанкционированной активности;
- во время анализа используются различные методы обнаружения атак: сигнатурный и поведенческий, а также идентификация аномалий в протоколах;
- система IPS в состоянии блокировать вредоносный трафик.

Таким образом, чтобы получить систему IPS из IDS, надо не только заменить одну букву в названии, но и изменить принципы работы решения, добавив новые технологии.

При рассмотрении IPS применяют классификацию, унаследованную от систем обнаружения вторжений, - деление средств предотвращения вторжений на сетевые и хостовые.

Сетевая система NIPS (*network-based IPS*) представляет средство предотвращения вторжений сетевого уровня, которое находится на пути передачи сетевого трафика и осуществляет его мониторинг. Основная задача сетевой NIPS - защита группы хостов сети от возможных атак путем анализа передаваемого трафика и блокирования трафика, связанного с проведением атак.

Хостовая система HIPS (*host-based IPS*) - это средство предотвращения вторжений уровня хоста, которое располагается на конкретном хосте и обеспечивает его защиту от разрушающих воздействий путем анализа сетевого трафика, поведения приложений, активируемых системных вызовов и т.п.

В системе предотвращения вторжений IPS выделяют также *средства защиты от распределенных атак типа «отказ в обслуживании» DDoS (Distributed Denial of Service)*.

Во многих средствах защиты сегодня объединены возможности обнаружения и блокирования вторжений, поэтому иногда их условно называют продуктами IDS/IPS.

Однако для эффективной защиты применения только средств IPS оказывается недостаточно - желательно знать заранее слабые места (уязвимости) КИС, называемые в обиходе «дырами», через которые злоумышленники могут успешно осуществить атаку. «Дырами» могут стать «слабые» пароли, несоответствия в настройках сетевых устройств, уязвимости операционных систем и приложений и т.п. Для

поиска и выявления таких уязвимостей существуют специализированные средства - *сканеры уязвимости (vulnerability assessment)*. Их использование в КИС существенно повышает уровень защиты: определив слабые места, администратор безопасности может предпринять соответствующие меры по их устранению до того, как злоумышленник воспользуется ими. В последнее время стали появляться специализированные средства, которые обеспечивают автоматический процесс устранения уязвимостей, но пока подобные решения предлагают немногие производители.

Чтобы максимально снизить риск негативного воздействия атак, необходимо объединить средства IPS, сканеры уязвимости и средства устранения уязвимостей в единую подсистему с централизованным управлением.

Решение по предотвращению вторжений состоит из сенсоров, одного или нескольких серверов управления, сканеров уязвимости, средств устранения уязвимостей, консоли оператора и администраторов (рис.8.1) [1].

Рис.8.1. Подсистема предотвращения вторжений в КИС (ДМЗ - демилитаризованная зона)

Иногда выделяется внешняя база данных для хранения информации о событиях информационной безопасности и их параметров.

Сканеры уязвимости осуществляют поиск и выявление уязвимостей в КИС. Сервер управления получает информацию от сенсоров обнаружения атак и управляет ими. Обычно на серверах осуществляется консолидация и корреляция событий. Для более глубокой обработки важных событий средства предотвращения вторжений системного уровня интегрируются с подсистемой мониторинга и управления инцидентами.

Консоли представляют интерфейсы для операторов и администраторов подсистемы. Обычно это программное средство, устанавливаемое на рабочей станции. Для организации централизованного администрирования, управления обновлениями сигнатур, управления конфигурациями применяется интеграция с подсистемой управления средствами защиты организации.

Необходимо учитывать, что только комплексное использование разных типов средств подсистемы позволяет достигнуть всестороннего и точного обнаружения и предотвращения вторжений.

8.2. Обнаружение вторжений системой IPS

В процессе выявления вторжений используются следующие методы анализа событий:

- обнаружение аномального поведения (anomaly-based), при котором определяются аномальные (ненормальные) события;
- обнаружение злоупотреблений (misuse detection или signature-based), при котором событие или множество событий проверяются на соответствие заранее определенному образцу (шаблону), описывающему известную атаку. Шаблон известной атаки называется сигнатурой.

8.2.1. Обнаружение аномального поведения

Технология обнаружения атак путем идентификации *аномального поведения* (*anomaly-based*) основана на следующей гипотезе. Аномальное поведение пользователя (т.е. атака или какое-нибудь враждебное действие) часто проявляется как отклонение от нормального поведения. При попытке вторжения

полученные события отличаются от событий нормальной деятельности пользователей или взаимодействия узлов сети и могут, следовательно, быть определены.

Примером аномального поведения может служить большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора и т.п. Сенсоры собирают данные о событиях, создают шаблоны нормальной деятельности и используют различные метрики для определения отклонения от нормального состояния.

Если можно было бы однозначно описать профиль нормального поведения пользователя, то любое отклонение от него можно идентифицировать как аномальное поведение. Однако аномальное поведение не всегда является атакой. Например, одновременную посылку большого числа запросов от администратора сети подсистема обнаружения атак может идентифицировать как атаку типа «отказ в обслуживании» («denial of service»).

При использовании такой технологии возможны два крайних случая:

- обнаружение аномального поведения, которое не является атакой, и отнесение его к классу атак;
- пропуск атаки, которая не подпадает под определение аномального поведения.

Второй случай более опасен, чем ложное отнесение аномального поведения к классу атак.

При настройке и эксплуатации систем этой категории администраторы сталкиваются со следующими проблемами:

- построение профиля пользователя является трудно формализуемой и трудоемкой задачей, требующей от администратора большой предварительной работы;
- определение граничных значений характеристик поведения пользователя для снижения вероятности появления одного из двух вышеназванных крайних случаев.

Технология обнаружения аномалий ориентирована на выявление новых типов атак. Однако ее недостаток - необходимость постоянного обучения. Пока технология обнаружения аномалий не получила широкого распространения, так как она трудно реализуема на практике. Однако сейчас наметился определенный интерес к ней.

8.2.2. Обнаружение злоупотреблений

Суть другого подхода к обнаружению атак - *обнаружение злоупотреблений* (*misuse detection* или *signature-based*) - заключается в описании атаки в виде сигнатуры (signature) и поиска данной сигнатуры в контролируемом пространстве (сетевом трафике или журнале регистрации).

В качестве сигнатуры атаки может выступать шаблон действий или строка символов, характеризующие аномальную деятельность. Эти сигнатуры хранятся в базе данных, аналогичной той, которая используется в антивирусных системах. Следует заметить, что антивирусные резидентные мониторы являются частным случаем подсистемы обнаружения атак, но поскольку эти направления изначально развивались параллельно, то принято разделять их. Поэтому данная технология обнаружения атак очень похожа на технологию обнаружения вирусов, при этом система может обнаружить все известные атаки. Однако системы данного типа не могут обнаруживать новые, еще неизвестные виды атак.

Подход, реализованный в таких системах, достаточно прост и именно на нем основаны практически все системы обнаружения атак.

Однако при эксплуатации и этих систем администраторы сталкиваются с проблемами. Первая проблема заключается в создании механизма описания сигнатур, т.е. языка описания атак. Вторая проблема, связанная с первой, заключается в том, как описать атаку, чтобы зафиксировать все возможные ее модификации.

Следует отметить, что для достоверного обнаружения факта вторжения не достаточно найти некий характерный шаблон трафика, или «сигнатуру». Для успешного обнаружения вторжений современная IPS должна обладать следующими свойствами и функциями:

- использовать знания о топологии защищаемой сети;
- проводить анализ сеанса взаимодействия с учетом протоколов, используемых для передачи данных;
- выполнять восстановление фрагментированных IP-пакетов до их анализа, не передавать фрагменты IP-датаграмм без проверки;
- отслеживать попытки создания перекрывающихся фрагментов IP-датаграмм, попытки перезаписи содержимого TCP-сегментов и предотвращать их;
- обеспечивать проверку соответствия логики/форматов работы по протоколу соответствующим RFC;
- выполнять статистический анализ данных;
- поддерживать механизмы сигнатурного поиска;
- обладать возможностью обучения и самообучения.

Кроме того, поскольку IPS может принимать решения о блокировании трафика, необходимо обеспечить надежное и безопасное удаленное управление IPS.

Средства конфигурирования IPS должны быть удобны для конечных пользователей. Большинство IPS поддерживают возможность задания «пользовательских» правил обнаружения вторжений для возможности подстройки IPS под конкретную среду или требования конкретного заказчика.

8.3. Предотвращение вторжений в КИС

Система обнаружения и предотвращения вторжений IPS охватывает решения следующих задач:

- предотвращение вторжений системного (хостового) уровня;
- предотвращение вторжений сетевого уровня;
- защита от DDoS-атак.

8.3.1. Предотвращение вторжений системного уровня

Средства предотвращения вторжений системного (хостового) уровня HIPS (Host-based IPS) действуют на уровне информационных узлов. Подсистема HIPS обеспечивает незамедлительное блокирование атак системного уровня и оповещение ответственных лиц.

Агенты (локальные сенсоры) обнаружения атак системного уровня собирают информацию, отражающую деятельность, которая происходит в отдельном информационном узле. Средства HIPS анализируют файлы журнала и ведут мониторинг пользовательской, сетевой и системной активности на узле информационной системы.

Логически локальные сенсоры устанавливаются между ядром ОС и пользовательским приложением. Локальные сенсоры перехватывают вызовы, обращенные к системе, сопоставляют их с правилами доступа, определенными политикой безопасности, и затем разрешают или запрещают доступ к ресурсам. Некоторые локальные сенсоры сличают запросы с БД известных сигнатур атак или аномального поведения.

Преимуществами данной подсистемы являются возможность контроля доступа к информационным объектам узла, проверка их целостности, регистрация аномальной деятельности конкретного пользователя.

К недостаткам можно отнести невозможность обнаружения комплексных аномальных событий, необходимость установки средств HIPS на все защищаемые узлы. Кроме того, уязвимости операционной системы могут нарушить целостность и работу сенсоров.

Средства предотвращения вторжений системного (хостового) уровня HIPS могут быть установлены на рабочей станции или сервере. При этом IPS уровня хоста реализуется несколькими способами:

- в виде программного обеспечения, интегрированного в операционную систему. Пока все решения ограничиваются ОС семейства UNIX;
- в виде прикладного ПО, устанавливаемого на рабочей станции или сервере «поверх» операционной системы. Выпускается многими производителями: Cisco Systems, ISS, McAfee, Star Force и др. Кроме отражения сетевых атак, такие IPS обладают еще большим количеством полезных функций: контроль доступа к USB, создание замкнутой программной среды, контроль утечки информации, контроль загрузки с посторонних носителей и т.д.;
- система IPS может представлять собой отдельную подсистему отражения атак, реализованную в сетевой карте. Некоторые производители (в частности, D-Link) выпускают такого рода устройства, однако их распространенность не велика [14].

8.3.2. Предотвращение вторжений сетевого уровня

Подсистема предотвращения вторжений сетевого уровня NIPS (network-based IPS) обеспечивает немедленное блокирование сетевых атак и оповещение ответственных лиц. Преимуществом применения средств сетевого уровня является возможность защиты одним средством сразу нескольких узлов или сегментов сети.

Программные или программно-аппаратные средства Network IPS (сетевые сенсоры) анализируют сетевой трафик определенных узлов или сегментов сети, а также сетевые, транспортные и прикладные протоколы взаимодействия.

Для обнаружения вторжения используется либо сравнение битовой последовательности проходящего потока данных с эталонным образцом (сигнатурой) атаки, либо фиксация подозрительной (аномальной) сетевой активности посредством анализа сетевого трафика или нарушений правил политики безопасности. В случае обнаружения попыток атаки применяются меры противодействия, в качестве которых могут выполняться:

- блокирование выбранных сетевых пакетов;
- изменение конфигурации средств других подсистем обеспечения информационной безопасности (например, межсетевого экрана) для более эффективного предотвращения вторжения;
- сохранение выбранных пакетов для последующего анализа;
- регистрация событий и оповещение ответственных лиц.

Дополнительной возможностью данных средств является сбор информации о защищаемых узлах. Для получения информации о защищенности и критичности узла или сегмента сети применяется интеграция с подсистемой контроля эффективности защиты информации.

IPS сетевого уровня могут быть реализованы как:

- выделенные аппаратные устройства (security appliance), которые могут быть установлены на периметре корпоративной сети и в ряде случаев внутри нее. Такие устройства - наиболее распространенный вариант. Основными производителями таких средств являются компании Cisco Systems, ISS, Juniper, 3Com, McAfee и др.;
- решения, интегрированные в инфраструктуру корпоративной сети.

Решения, интегрированные в инфраструктуру, гораздо эффективнее выделенных аппаратных устройств:

- стоимость интегрированного решения ниже стоимости автономного (stand-alone) устройства;
- ниже и стоимость внедрения (финансовая и временная) такого решения - можно не менять топологию сети;
- надежность выше, так как в цепочке прохождения трафика отсутствует дополнительное звено, подверженное отказам;
- интегрированные решения предоставляют более высокий уровень защиты за счет более тесного взаимодействия с защищаемыми ресурсами.

Сама интеграция может быть выполнена различными путями:

- *использование маршрутизатора (router)* - самый распространенный способ. В этом случае система IPS становится составной частью данного устройства и получает доступ к анализируемому трафику сразу после поступления его на определенный интерфейс. Система IPS может быть реализована в виде отдельного модуля, вставляемого в шасси маршрутизатора, или в виде неотъемлемой части операционной системы маршрутизатора. Первой в данном направлении развития систем IPS стала компания Cisco Systems. Однако система IPS, интегрированная в маршрутизатор, умеет отражать атаки только на периметре сети, оставляя внутренние ресурсы без защиты;
- *использование коммутаторов локальной сети (switch)*, в которые могут быть внедрены механизмы предотвращения атак, причем как в виде части ОС, так и в виде отдельного аппаратного модуля. Эту технологию интеграции IPS в коммутаторы реализовала Cisco Systems в своем семействе Cisco Catalyst;
- *использование точек беспроводного доступа (wireless access point)*, через которые может проходить трафик, нуждающийся в анализе. По пути интеграции пошли такие производители, как Cisco Systems и Aruba, оснастившие свое оборудование необходимыми функциями. Такие системы, помимо обнаружения и предотвращения различных атак, умеют определять местонахождение несанкционированно установленных беспроводных точек доступа и клиентов [14].

Пример схемы предотвращения вторжений сетевого уровня на основе продуктов Cisco Systems приведен на рис.8.2 [19].

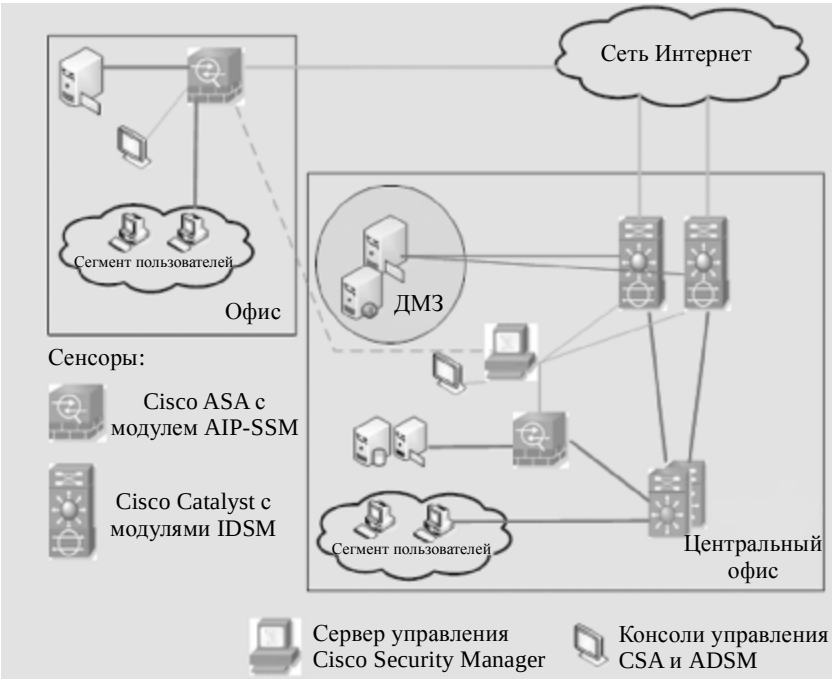

Рис.8.2. Схема предотвращения вторжений сетевого уровня на основе продуктов компании Cisco Systems

Сравнительная характеристика подсистем Network IPS и Host IPS приведена в табл.8.1 [14].

Таблица 8.1

Сравнительная характеристика подсистем Network IPS и Host IPS

Достоинства	Недостатки
Network IPS	
Широта применения - целая сеть может быть «покрыта» одним сетевым сенсором. Минимальные неудобства от установки обновлений сигнатур и обновлений ПО сенсоров. Предотвращение DoS-атаки. Возможность обнаружения ошибок сетевого уровня в стеке TCP/IP. Независимость от ОС информационных узлов	Наряду с верными бывают и ложные срабатывания. Не может анализировать зашифрованный поток данных. Новые виды или варианты атак не будут выявлены в случае отсутствия сигнатуры данной атаки. Задержка во времени между моментом обнаружения атаки и моментом оповещения (тревоги). Затруднен анализ пакетов в случае перегруженной сети. Отсутствуют уведомления об успешности атаки
Host IPS	
Возможность связывать пользователя с событием. Могут обнаруживать атаки, не обнаруженные сенсорами NIDS. Могут проводить анализ данных, расшифрованных на узле. Возможность предоставления информации об узле в течение атаки на него	Для защиты нескольких узлов сенсоры должны быть установлены на каждом из них. Если ОС «взломана» в результате атаки, то перестает функционировать и сенсор, установленный на данном узле. Сенсор не способен обнаруживать деятельность сетевых сканеров. Сенсоры могут быть неэффективными в случае DoS-атаки на узел. Для функционирования необходимы дополнительные ресурсы

8.3.3. Защита от DDoS-атак

Одним из наиболее критичных, по последствиям, классов компьютерных атак являются распределенные атаки типа «отказ в обслуживании» DDoS (Distributed Denial of Service), направленные на нарушение доступности информационных ресурсов. Эти атаки осуществляются с использованием множества программных компонентов, размещаемых на хостах в сети Интернет. Они могут привести не только к выходу из строя отдельных узлов и сервисов, но и остановить работу корневых DNS-серверов и вызвать частичное или полное прекращение функционирования сети.

Основная цель защиты против DDoS-атак заключается в предотвращении их реализации, точном обнаружении этих атак и быстром реагировании на них. При этом важно также эффективно распознавать легитимный трафик, который имеет признаки, схожие с трафиком вторжения, и обеспечивать надежную доставку легитимного трафика по назначению.

Общий подход к защите от DDoS-атак включает реализацию следующих механизмов:

- обнаружение вторжения;
- определение источника вторжения;
- предотвращение вторжения.

При разработке *системы защиты предприятий от DDoS-атак* необходим комплексный подход, способный защитить не только отдельные серверы предприятия, но и каналы связи с соответствующими операторами связи. Решение представляет собой многоуровневую систему с четко выстроенной линией обороны. Внедрение решения позволяет повысить защищенность корпоративной сети, устройств маршрутизации, канала связи, почтовых серверов, Web-серверов и DNS-серверов [19].

Внедрение такой системы защиты целесообразно в случаях:

- осуществления компаниями своего бизнеса через Интернет;
- наличия корпоративного Web-сайта компании;

- использования сети Интернет для реализации бизнес-процессов.

Схема защиты предприятия от DDoS-атак представлена на рис.8.3.

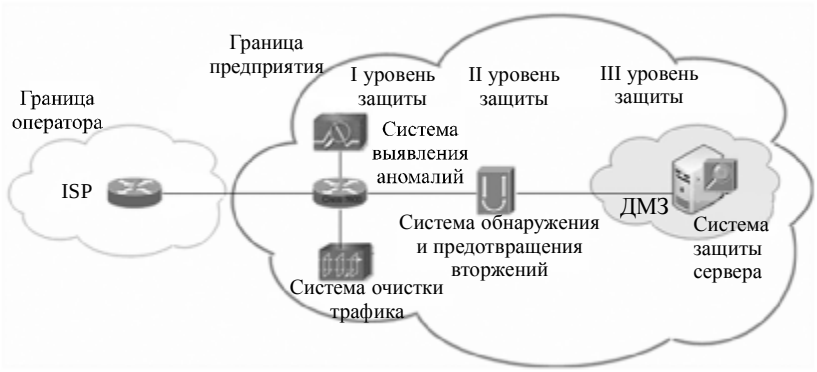

Рис.8.3. Схема защиты предприятий от DDoS-атак

В данном решении применяются сенсоры обнаружения аномалий, просматривающие проходящий внешний трафик в непрерывном режиме. Данная система находится на границе с оператором связи, таким образом, процесс очистки начинается еще до попадания трафика атаки во внутреннюю сеть компании.

Метод обнаружения аномалий не может обеспечить 100% вероятность очистки трафика, поэтому появляется необходимость интеграции с подсистемами предотвращения атак на сетевом и системном уровне.

8.4. Современные средства предотвращения вторжений

Компания Cisco Systems, признанный лидер в области сетевых решений, предлагает широкий выбор продуктов в области обеспечения информационной безопасности - от межсетевых экранов и систем предотвращения атак до защиты приложений и систем персональной защиты серверов и рабочих станций. Рассмотрим два продукта компании Cisco Systems, предназначенных для предотвращения вторжений.

Модуль обнаружения и отражения атак Cisco IDS/IPS. Модуль Cisco IDS/IPS является центральным компонентом решений Cisco Systems по отражению атак. Наряду с традиционными механизмами в Cisco IDS/IPS используются и уникальные алгоритмы, отслеживающие аномалии в сетевом трафике и отклонения от нормального поведения сетевых приложений. Это позволяет обнаруживать как известные, так и многие неизвестные атаки.

Встроенные технологии корреляции событий безопасности Cisco Threat Response, Threat Risk Rating и Meta Event Generator не только помогают существенно снизить число ложных срабатываний, но и позволяют администраторам реагировать лишь на действительно критичные атаки, которые могут нанести серьезный ущерб ресурсам корпоративной сети.

Перечислим основные возможности данного модуля:

- широкий спектр алгоритмов обнаружения атак (сигнатуры, аномалии, эвристика, отклонения от RFC и т.п.);
- защита от методов обхода;
- возможность работы одновременно в двух режимах - обнаружения и предотвращения атак;
- обнаружение атак на IP-телефонию и АСУ ТП (SCADA);
- автоматический выбор реагирования в зависимости от степени угрозы;
- производительность составляет 8 Гбит/с в кластере;
- интеграция с Cisco Incident Control System;
- обнаружение атак в инкапсулированном трафике MPLS, GRE, IPv6, Mobile IP-in-IP;
- интеграция с Cisco PIX/Cisco ASA 5500 и Cisco Secuirty Agent для блокирования атак;
- поддержка нескольких виртуальных сенсоров на одном устройстве;
- интеграция с коммутаторами и маршрутизаторами для блокирования атак путем изменения ACL или ограничения скорости передачи трафика (Rate Limiting);
- возможность распределения нагрузки между несколькими сенсорами и обеспечение отказоустойчивости;
- выборочное блокирование (не всего IP-адреса, а только атакующего сервиса);
- поддержка до 255 VLAN на один интерфейс сенсора;

- возможность эффективного предотвращения атак в коммутируемых сетях;
- импорт данных от сканеров безопасности;
- механизм OS Fingerprint для определения релевантности атаки;
- оценка эффективности реагирования на атаку.

Существует ряд моделей Cisco IDS/IPS: IDS 4215, IPS 4240, IPS 4255, IDS 4260, которые различаются по производительности (от 65 до 1000 Мбит/с) и интерфейсу для мониторинга.

Система Cisco Guard и Traffic Anomaly Detector. Cisco Guard позволяет отражать атаки типа «отказ в обслуживании» DoS, в том числе и распределенные DDoS, идентифицированные специализированными средствами обнаружения вторжений, в качестве которых могут выступать Cisco Anomaly Traffic Detector и Cisco IDS/IPS 42xx. Блокирование основано на технологии многоступенчатой проверки, которая позволяет блокировать вредоносные информационные потоки и пропускать те, которые содержат легитимные транзакции, несущие полезные данные.

Основные возможности данных систем:

- уникальная архитектура Multiverification Process (MVP);
- отсутствие снижения производительности защищаемой сети;
- скорость обработки трафика составляет 3 Гбит/с (возможность масштабирования до 30 Гбит/с путем использования кластера из 10 Cisco Guard);
- число параллельно обрабатываемых соединений равно 4,5 млн;
- возможность поставки в виде выделенного устройства или модуля для коммутатора Cisco Catalyst 6500 или маршрутизатора Cisco 7600;
- защита от одновременной атаки со стороны свыше 100 000 зомби (механизм Zombie Killer);
- число динамических фильтров - 150 000 (добавление 1000 фильтров в секунду);
- задержка - менее 1 м/с;
- централизованное управление и интеграция с CiscoWorks SIMS;
- соблюдение необходимого уровня SLA;
- обеспечение услуг аутсорсинга;
- защита от DoS-атак на IP-телефонию (SIP);
- технология обнаружения подозрительного трафика путем профилирования нормального поведения в режиме самообучения и обнаружения аномалий;
- поддержка до 500 зон безопасности с различными политиками безопасности (одновременно защищаются до 50 зон).

Вопросы для самоконтроля

1. Сформулируйте понятия: обнаружение вторжений и предотвращение вторжений.
2. Укажите четыре признака системы IPS, отличающие ее от системы IDS.
3. Дайте определения понятий: сетевая система NIPS (network-based IPS) и хостовая система HIPS (host-based IPS).
4. Сформулируйте назначение и особенности применения специализированных средств - сканеров уязвимости (vulnerability assessment).
5. Какие методы анализа событий используются в процессе выявления вторжений?
6. В чем суть метода обнаружения аномального поведения?
7. В чем суть метода обнаружения злоупотреблений?
8. Опишите функциональность средств предотвращения вторжений системного (хостового) уровня HIPS (Host-based IPS).
9. Опишите функциональность средств предотвращения вторжений сетевого уровня NIPS (network-based IPS).
10. Сформулируйте подход к защите от распределенных атак типа «отказ в обслуживании» DDoS (Distributed Denial of Service).
11. Какими свойствами и функциями должна обладать современная IPS для успешного обнаружения и предотвращения вторжений?
12. Опишите структуру и функционирование подсистемы предотвращения вторжений в КИС.

Глава 9. Межсетевое экранирование

Сражаясь с тем, кто умеет обороняться,
противник не знает, где ему нападать.

Сунь-цзы. «Трактат о военном искусстве»

Межсетевое экранирование является одним из важных элементов эшелонированной обороны корпоративной сети.

Межсетевой экран - это специализированный комплекс межсетевой защиты, называемый также системой *firewall* или брандмауэром. Межсетевой экран позволяет разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Интернет.

Обычно межсетевые экраны защищают внутреннюю сеть предприятия от «вторжений» из глобальной сети Интернет, хотя они могут использоваться и для защиты от «нападений» из корпоративной интрасети, к которой подключена локальная сеть предприятия.

Для большинства организаций установка межсетевого экрана является необходимым условием обеспечения безопасности внутренней сети.

9.1. Функции межсетевых экранов

Для противодействия несанкционированному межсетевому доступу межсетевой экран МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис.9.1). При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран.

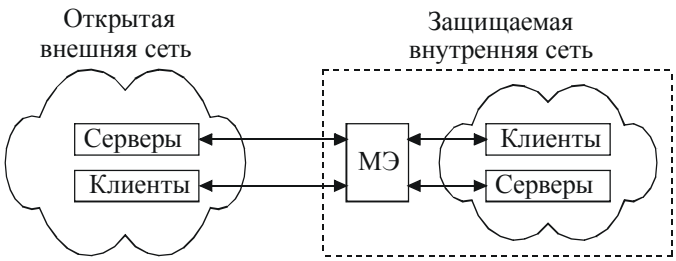

Рис.9.1. Схема подключения межсетевого экрана

Межсетевой экран, защищающий сразу множество узлов внутренней сети, должен решить две основные задачи:

- ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи и хакеры;
- разграничение доступа пользователей защищаемой сети к внешним ресурсам.

До сих пор не существует единой общепризнанной классификации межсетевых экранов.

МЭ можно классифицировать по следующим основным признакам [3]:

- *по функционированию на уровнях модели взаимодействия открытых систем OSI (Open Systems Interconnection)* [1]:

- пакетный фильтр *(*экранирующий маршрутизатор - *screening router),*
- шлюз сеансового уровня (экранирующий транспорт),
- прикладной шлюз *(application gateway),*
- шлюз экспертного уровня *(stateful inspection firewall);*

- *по используемой технологии:*

- контроль состояния протокола *(stateful inspection),*
- на основе модулей посредников *(proxy);*

- *по исполнению:*

- аппаратно-программный,
- программный;

- *по схеме подключения:*

- схема единой защиты сети,
- схема с защищаемым закрытым и незащищаемым открытым сегментами сети,

- схема с раздельной защитой закрытого и открытого сегментов сети.

9.1.1. Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно с выполнением некоторых преобразований [1, 3]. Фильтрация осуществляется на основе набора предварительно загруженных в межсетевой экран правил, соответствующих принятой политике безопасности. Поэтому межсетевой экран удобно представлять как последовательность фильтров, обрабатывающих информационный поток (рис.9.2).

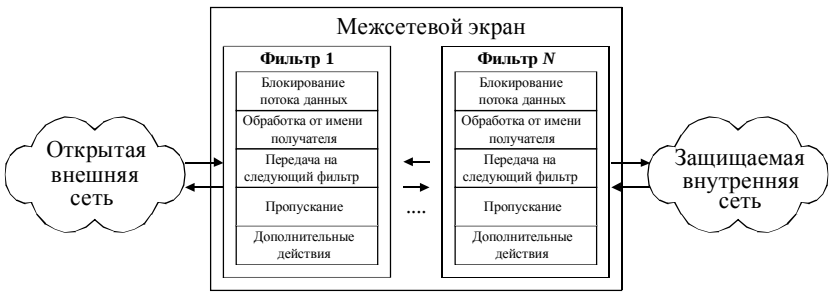

Рис.9.2. Структура межсетевого экрана

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих действий:

1. Анализ информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена.
2. Принятие на основе интерпретируемых правил одного из следующих решений:

- не пропустить данные;
- обработать данные от имени получателя и возвратить результат отправителю;
- передать данные на следующий фильтр для продолжения анализа;
- пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрация событий и др. Соответственно правила фильтрации определяют перечень условий, по которым осуществляется:

- разрешение или запрещение дальнейшей передачи данных;
- выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

- служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
- непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
- внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т.д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация.

9.1.2. Выполнение функций посредничества

Шлюз сеансового уровня, называемый еще экранирующим транспортом, функционирует в основном на сеансовом уровне модели OSI. Защитные функции шлюза сеансового уровня относятся к функциям посредничества. *Прикладной шлюз*, называемый также экранирующим шлюзом, функционирует в основном на прикладном уровне модели OSI. Защитные функции прикладного шлюза, как и шлюза сеансового уровня, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять большее количество функций защиты.

Функции посредничества МЭ выполняет с помощью специальных программ, называемых *программами-посредниками*. Данные программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере МЭ. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного

посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

Следует иметь в виду, что МЭ может выполнять функции фильтрации без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетью. В общем случае *программы-посредники*, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:

- проверку подлинности передаваемых данных;
- фильтрацию и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- кэширование данных, запрашиваемых из внешней сети;
- идентификацию и аутентификацию пользователей;
- трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
- регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов [1, 3].

Программы-посредники могут осуществлять *проверку подлинности получаемых и передаваемых данных*. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей.

Программы-посредники могут выполнять *разграничение доступа к ресурсам внутренней или внешней сети*, используя результаты идентификации и аутентификации пользователей при их обращении к межсетевому экрану.

При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих подходов:

- разрешение доступа только по заданным адресам во внешней сети;
- фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;
- накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти МЭ и полный запрет доступа во внешнюю сеть.

С помощью специальных посредников поддерживается также *кэширование данных*, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска МЭ, называемого в этом случае proxy-сервером. Поэтому, если при очередном запросе нужная информация окажется на proxy-сервере, посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил. Здесь следует различать два вида программ-посредников:

- экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например протоколы FTP, HTTP, Telnet;
- универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных, и если какой-либо объект не соответствует заданным критериям, то посредник либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например обезвреживание обнаруженных компьютерных вирусов. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы.

МЭ с посредниками позволяют также организовывать защищенные виртуальные сети VPN (Virtual Private Network), например безопасно объединить несколько локальных сетей, подключенных к Интернет, в одну виртуальную сеть.

Помимо выполнения фильтрации трафика и функций посредничества современные межсетевые экраны позволяют реализовать ряд других не менее важных функций, без которых обеспечение защиты периметра внутренней сети было бы неполным [1].

9.1.3. Дополнительные возможности МЭ

Рассмотрим реализацию межсетевыми экранами таких функций, как идентификация и аутентификация пользователей, трансляция внутренних сетевых адресов для исходящих пакетов сообщений, регистрация событий, реагирование на задаваемые события, анализ зарегистрированной информации и генерация отчетов.

Идентификация и аутентификация пользователей. Кроме разрешения или запрещения допуска различных приложений в сеть межсетевые экраны могут также выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам, разделяемым межсетевым экраном.

Прежде чем пользователю будет предоставлено право использовать какой-либо сервис, необходимо убедиться, что пользователь действительно тот, за кого себя выдает. Идентификация и аутентификация пользователей являются важными компонентами концепции межсетевых экранов. Авторизация пользователя обычно рассматривается в контексте аутентификации - как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы.

Идентификация и аутентификация пользователя иногда осуществляются при предъявлении обычного идентификатора (имени) и пароля. Однако эта схема уязвима с точки зрения безопасности - пароль может быть перехвачен и использован другим лицом. Многоразовый пароль следует передавать через общедоступные коммуникации в зашифрованном виде.

Более надежным методом аутентификации является использование одноразовых паролей. Широкое распространение получила технология аутентификации на основе одноразовых паролей SecurID, реализованная в коммуникационных серверах ряда компаний, в частности в серверах компании Cisco Systems и др.

Удобно и надежно также применение цифровых сертификатов, выдаваемых доверенными органами, например центром распределения ключей. Большинство программ-посредников разрабатываются таким образом, чтобы пользователь аутентифицировался только в начале сеанса работы с межсетевым экраном. После этого от него не требуется дополнительная аутентификация в течение времени, определяемого администратором.

Так как межсетевые экраны могут централизовать управление доступом в сети, они являются подходящим местом для установки программ или устройств усиленной аутентификации. Хотя средства усиленной аутентификации могут использоваться на каждом хосте, более практично их размещение на межсетевом экране. Ряд межсетевых экранов поддерживают Kerberos - один из распространенных методов аутентификации. Как правило, большинство коммерческих межсетевых экранов поддерживают несколько различных схем аутентификации, позволяя администратору сетевой безопасности сделать выбор наиболее приемлемой схемы для своих условий.

Трансляция сетевых адресов. Для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, межсетевые экраны выполняют очень важную функцию - трансляцию внутренних сетевых адресов NAT (network address translation). Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов выполняется автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP-адрес. IP-адрес МЭ становится единственным активным IP-адресом, который попадает во внешнюю сеть. В результате все исходящие из внутренней сети пакеты оказываются отправленными МЭ, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности, трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например в сети Интернет. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

Администрирование, регистрация событий и генерация отчетов. Простота и удобство администрирования являются одним из ключевых аспектов в создании эффективной и надежной системы защиты. Ошибки при определении правил доступа могут образовать «дыру», через которую может быть взломана система. Поэтому в большинстве межсетевых экранов реализованы сервисные утилиты, облегчающие ввод, удаление, просмотр набора правил.

Важными функциями межсетевых экранов являются *регистрация событий*, *реагирование на задаваемые события*, а также *анализ зарегистрированной информации и составление отчетов*. Являясь критическим элементом системы защиты корпоративной сети, межсетевой экран имеет возможность регистрации всех фиксируемых им действий. К таким действиям относятся не только пропуск или блокирование сетевых пакетов, но и изменение правил разграничения доступа администратором безопасности и другие действия. Такая регистрация позволяет обращаться к создаваемым журналам по мере необходимости - в случае возникновения инцидента безопасности или сбора доказательств для внутреннего расследования или для предоставления их в судебные инстанции. При правильно настроенной системе фиксации сигналов о подозрительных событиях (alarm) межсетевой экран может дать детальную информацию о том, были ли межсетевой экран или сеть атакованы или зондированы.

Многие МЭ содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей. Системы учета позволяют произвести анализ статистики и предоставляют администраторам подробные отчеты. За счет использования специальных протоколов МЭ могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, т.е. выдача предупредительных сигналов.

9.2. Особенности функционирования межсетевых экранов

Многие из широко используемых МЭ являются либо экранирующими маршрутизаторами, либо межсетевыми экранами экспертного уровня. Рассмотрим подробнее МЭ указанных типов.

9.2.1. Экранирующий маршрутизатор

Экранирующий маршрутизатор (screening router), называемый также *пакетным фильтром (packet filter),* предназначен для фильтрации пакетов сообщений и обеспечивает прозрачное взаимодействие между внутренней и внешней сетями. Он функционирует на сетевом уровне эталонной модели OSI, но для выполнения своих отдельных функций может охватывать и транспортный уровень эталонной модели [1].

Решение о том, пропустить или отбраковать данные, принимается для каждого пакета независимо на основе заданных правил фильтрации. Для принятия решения анализируются заголовки пакетов сетевого и транспортного уровней (рис.9.3).

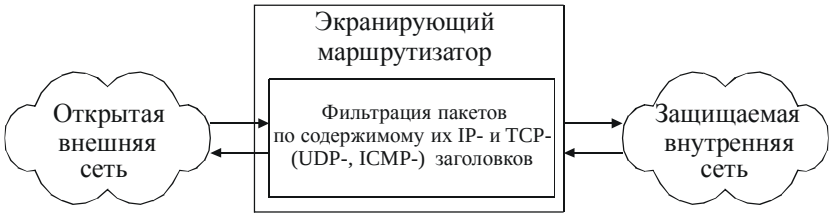

Рис.9.3. Схема функционирования пакетного фильтра

В качестве анализируемых полей заголовков каждого пакета могут использоваться:

- адрес отправителя;
- адрес получателя;
- тип пакета;
- флаг фрагментации пакета;
- номер порта источника;
- номер порта получателя.

Адреса отправителя и получателя являются IP-адресами. Эти адреса заполняются при формировании пакета и остаются неизменными при передаче его по сети. Поле типа пакета содержит код используемого протокола. Флаг фрагментации пакета определяет наличие или отсутствие фрагментации IP-пакетов. Номера портов источника и получателя однозначно идентифицируют приложение-отправитель, а также приложение, для которого предназначен этот пакет.

При обработке каждого пакета экранирующий маршрутизатор последовательно просматривает заданную таблицу правил, пока не найдет правила, с которым согласуется полная ассоциация пакета. Здесь под ассоциацией понимается совокупность параметров, указанных в заголовках данного пакета. Если экранирующий маршрутизатор получил пакет, не соответствующий ни одному из табличных правил, он применяет правило, заданное по умолчанию. Из соображений безопасности это правило обычно указывает на необходимость отбраковки всех пакетов, не удовлетворяющих ни одному из других правил.

Пакетные фильтры могут быть реализованы как аппаратно, так и программно. В качестве пакетного фильтра могут быть использованы как обычный маршрутизатор, так и работающая на сервере программа, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты.

Современные маршрутизаторы, в частности компании Cisco, позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе.

Обладая рядом положительных качеств, пакетные фильтры не лишены недостатков. Они не обеспечивают высокой степени безопасности, так как проверяют только заголовки пакетов и не поддерживают многие необходимые функции защиты, например аутентификацию конечных узлов, криптографическое закрытие пакетов сообщений, а также проверку их целостности и подлинности. Пакетные фильтры уязвимы для таких распространенных сетевых атак, как подмена исходных адресов и несанкционированное изменение содержимого пакетов сообщений.

Однако такие достоинства пакетных фильтров, как простота реализации, высокая производительность, прозрачность для программных приложений и малая цена, обусловленная тем, что любой маршрутизатор в той или иной степени предоставляет возможность фильтрации пакетов, перевешивают указанные недостатки и обусловливают их повсеместное распространение и использование как обязательного элемента системы сетевой безопасности. Кроме того, они являются составной частью практически всех межсетевых экранов, использующих контроль состояния.

9.2.2. Межсетевые экраны экспертного уровня

Межсетевые экраны, в основу функционирования которых положена фильтрация пакетов *с контролем состояния соединения (stateful inspection)* или, иными словами, фильтрация экспертного уровня, называют *МЭ экспертного уровня*.

Технология фильтрации пакетов *с контролем состояния соединения (stateful inspection)* разработана компаниями Check Point и ON Technology [1]. Такая фильтрация осуществляется на основе специальных методов многоуровневого анализа состояния пакетов SMLT (Stateful Multi-Layer Technique).

Эта гибридная технология позволяет отслеживать состояние сетевого соединения, перехватывая пакеты на сетевом уровне и извлекая из них информацию прикладного уровня, которая используется для контроля за соединением. Быстрое сравнение проходящих пакетов с известным состоянием *(state)* «дружественных» пакетов позволяет значительно сократить время обработки по сравнению с МЭ уровня приложений.

МЭ экспертного уровня сочетают в себе элементы экранирующих маршрутизаторов и прикладных шлюзов. Как и экранирующие маршрутизаторы, они обеспечивают фильтрацию пакетов по содержимому их заголовков сетевого и транспортного уровней модели OSI. МЭ экспертного уровня также выполняют все функции прикладного шлюза, касающиеся фильтрации пакетов на прикладном уровне модели OSI. Они оценивают содержимое каждого пакета в соответствии с заданной политикой безопасности.

Таким образом, МЭ экспертного уровня позволяют контролировать:

- каждый передаваемый пакет - на основе имеющейся таблицы правил;
- каждую сессию - на основе таблицы состояний;
- каждое приложение - на основе разработанных посредников.

Достоинством межсетевых экранов экспертного уровня является «прозрачность» для конечного пользователя, не требующая дополнительной настройки или изменения конфигурации клиентского программного обеспечения. Помимо прозрачности для пользователей и более высокой скорости обработки информационных потоков к достоинствам межсетевых экранов экспертного уровня относится также то, что эти МЭ не изменяют IP-адресов проходящих через них пакетов. Это означает, что любой протокол прикладного уровня, использующий IP-адреса, будет корректно работать с этими МЭ без каких-либо изменений или специального программирования.

Поскольку данные МЭ допускают прямое соединение между авторизованным клиентом и компьютером внешней сети, они обеспечивают менее высокий уровень защиты. Поэтому на практике технология фильтрации экспертного уровня используется для повышения эффективности функционирования комплексных МЭ. Примером МЭ, реализующего технологию фильтрации экспертного уровня, является Firewall-1 компании Check Point Software. Следует заметить, что термин «stateful inspection», введенный компанией Check Point Software, стал таким популярным, что сейчас трудно найти межсетевой экран, который бы не относили к этой категории.

В настоящее время фильтрация экспертного уровня становится одной из функций новых маршрутизаторов. Например, компания Cisco Systems разработала собственную технологию МЭ экспертного уровня и реализовала ее в продукте Cisco PIX Firewall.

9.2.3. Варианты исполнения межсетевых экранов

Существует два основных варианта исполнения межсетевых экранов - программный и программно-аппаратный. В свою очередь, программно-аппаратный вариант исполнения межсетевых экранов имеет две разновидности - в виде специализированного устройства и в виде модуля в маршрутизаторе или коммутаторе.

В настоящее время чаще используется программное решение, которое, на первый взгляд, выглядит более привлекательным. Это связано с тем, что для его применения достаточно, казалось бы, только приобрести программное обеспечение межсетевого экрана и установить на любой компьютер, имеющийся в организации. Однако на практике далеко не всегда в организации находится свободный компьютер, да еще и удовлетворяющий достаточно высоким требованиям по системным ресурсам. Поэтому одновременно с приобретением программного обеспечения приобретается и компьютер для его установки.

В последние годы возрос интерес к программно-аппаратным решениям [1, 14]. Такие решения начинают постепенно вытеснять «чисто» программные системы. Все более широкое распространение стали получать специализированные программно-аппаратные решения, называемые *security appliance*. Программно-аппаратный комплекс межсетевого экранирования обычно состоит из компьютера, а также функционирующих на нем операционной системы и специального программного обеспечения. Это специальное программное обеспечение часто называют firewall. Используемый компьютер должен быть достаточно мощным и физически защищенным, например находиться в специально отведенном и охраняемом помещении. Кроме того, он должен иметь средства защиты от загрузки ОС с несанкционированного носителя. Программно-аппаратные комплексы используют специализированные или обычные операционные системы (как правило, на базе FreeBSD, Linux или Microsoft Windows), «урезанные» для выполнения заданных функций и удовлетворяющие ряду требований:

- иметь средства разграничения доступа к ресурсам системы;
- блокировать доступ к компьютерным ресурсам в обход предоставляемого программного интерфейса;

- запрещать привилегированный доступ к своим ресурсам из локальной сети;
- содержать средства мониторинга/аудита любых административных действий.

Специализированные программно-аппаратные решения обладают следующими достоинствами:

- *простота внедрения в технологию обработки информации* - такие средства поставляются уже с заранее установленной и настроенной операционной системой и защитными механизмами, поэтому необходимо только подключить их к сети, что выполняется в течение нескольких минут;
- *простота управления* - данные средства могут управляться с любой рабочей станции Windows или Unix. Взаимодействие консоли управления с устройством осуществляется либо по стандартным протоколам, например, Telnet или SNMP, либо при помощи специализированных или защищенных протоколов, например, SSH или SSL;
- *отказоустойчивость и высокая доступность* - исполнение межсетевого экрана в виде специализированного программно-аппаратного комплекса позволяет реализовать механизмы обеспечения не только программной, но и аппаратной отказоустойчивости и высокой доступности;
- *высокая производительность и надежность* - за счет исключения из операционной системы всех «ненужных» сервисов и подсистем, программно-аппаратный комплекс работает более эффективно с точки зрения производительности и надежности;
- *специализация на защите* - решение только задач обеспечения сетевой безопасности не приводит к затратам ресурсов на выполнение других функций, например маршрутизации и т.п.

9.3. Схемы сетевой защиты на базе межсетевых экранов

При подключении корпоративной или локальной сети к глобальным сетям необходимо решать следующие задачи:

- защита корпоративной или локальной сети от несанкционированного удаленного доступа со стороны глобальной сети;
- скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
- разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть.

Для эффективной защиты межсетевого взаимодействия система МЭ должна быть правильно установлена и сконфигурирована. Данный процесс состоит из следующих шагов:

- формирование политики межсетевого взаимодействия;
- выбор схемы подключения и настройка параметров функционирования межсетевого экрана.

9.3.1. Формирование политики межсетевого взаимодействия

Политика межсетевого взаимодействия является составной частью общей политики безопасности в организации. Политика межсетевого взаимодействия определяет требования к безопасности информационного обмена организации с внешним миром. Эта политика должна отражать два аспекта:

- политику доступа к сетевым сервисам;
- политику работы межсетевого экрана.

Политика доступа к сетевым сервисам определяет правила предоставления, а также использования всех возможных сервисов защищаемой компьютерной сети. В рамках данной политики должны быть заданы все сервисы, предоставляемые через межсетевой экран, и допустимые адреса клиентов для каждого сервиса. Кроме того, для пользователей должны быть указаны правила, описывающие, когда и какие пользователи каким сервисом и на каком компьютере могут воспользоваться.

Для того чтобы межсетевой экран успешно защищал ресурсы организации, политика доступа пользователей к сетевым сервисам должна быть реалистичной. Реалистичной считается такая политика, при которой найден баланс между защитой сети организации от известных рисков и необходимым доступом пользователей к сетевым сервисам.

Политика работы межсетевого экрана задает базовый принцип управления межсетевым взаимодействием, положенный в основу функционирования МЭ. Может быть выбран один из двух таких принципов:

- запрещено все, что явно не разрешено;
- разрешено все, что явно не запрещено.

Фактически выбор принципа устанавливает, насколько «подозрительной» или «доверительной» должна быть система защиты.

При выборе принципа «запрещено все, что явно не разрешено» межсетевой экран настраивается таким образом, чтобы блокировать любые явно не разрешенные межсетевые взаимодействия. Данный принцип соответствует классической модели доступа, используемой во всех областях информационной безопасности. Такой подход позволяет адекватно реализовать принцип минимизации привилегий, поэтому с точки зрения безопасности он является лучшим. Принцип «запрещено все, что явно не разрешено», в сущности, является

признанием факта, что незнание может причинить вред. Следует отметить, что правила доступа, сформулированные в соответствии с этим принципом, могут доставлять пользователям определенные неудобства.

При выборе принципа «разрешено все, что явно не запрещено» межсетевой экран настраивается таким образом, чтобы блокировать только явно запрещенные межсетевые взаимодействия. В этом случае повышается удобство использования сетевых сервисов со стороны пользователей, но снижается безопасность межсетевого взаимодействия.

Пользователи имеют больше возможностей обойти межсетевой экран, например, пользователи могут получить доступ к новым сервисам, не запрещаемым политикой (или даже не указанным в политике), или запустить запрещенные сервисы на нестандартных портах TCP/UDP, которые не запрещены политикой. Администратор может учесть не все действия, которые запрещены пользователям. Ему приходится работать в режиме реагирования, предсказывая и запрещая те межсетевые взаимодействия, которые отрицательно воздействуют на безопасность сети. При реализации данного принципа внутренняя сеть оказывается менее защищенной от нападений хакеров. Поэтому производители межсетевых экранов обычно отказываются от использования данного принципа.

Межсетевой экран не является симметричным. Для него отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю сеть и наоборот. В общем случае работа межсетевого экрана основана на динамическом выполнении двух групп функций:

- фильтрации проходящих через него информационных потоков;
- посредничества при реализации межсетевых взаимодействий.

9.3.2. Основные схемы подключения межсетевых экранов

При подключении корпоративной сети к глобальным сетям необходимо разграничить доступ в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть, а также обеспечить защиту подключаемой сети от несанкционированного удаленного доступа со стороны глобальной сети. При этом организация заинтересована в сокрытии информации о структуре своей сети и ее компонентов от пользователей глобальной сети. Работа с удаленными пользователями требует установления жестких ограничений доступа к информационным ресурсам защищаемой сети.

У организации часто возникает потребность иметь в составе корпоративной сети нескольких сегментов с разными уровнями защищенности:

- свободно доступные сегменты (например, рекламный WWW-сервер);
- сегмент с ограниченным доступом (например, для доступа сотрудникам организации с удаленных узлов);
- закрытые сегменты (например, финансовая локальная подсеть организации).

Для подключения межсетевых экранов могут использоваться различные схемы, которые зависят от условий функционирования защищаемой сети, а также от количества сетевых интерфейсов и других характеристик используемых МЭ. Широкое распространение получили следующие схемы подключения межсетевых экранов:

- схемы защиты сети с использованием экранирующего маршрутизатора;
- схемы единой защиты локальной сети;
- схемы с защищаемой закрытой и незащищаемой открытой подсетями;
- схемы с раздельной защитой закрытой и открытой подсетей [1, 3].

Схема защиты с использованием экранирующего маршрутизатора. Межсетевой экран, основанный на фильтрации пакетов, является самым распространенным и наиболее простым в реализации. Он состоит из экранирующего маршрутизатора, расположенного между защищаемой сетью и потенциально враждебной открытой внешней сетью (рис.9.4).

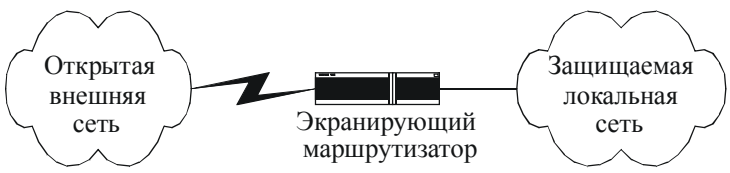

Рис.9.4. Межсетевой экран - экранирующий маршрутизатор

Экранирующий маршрутизатор (пакетный фильтр) сконфигурирован для блокирования или фильтрации входящих и исходящих пакетов на основе анализа их адресов и портов.

Компьютеры, находящиеся в защищаемой сети, имеют прямой доступ в сеть Интернет, в то время как большая часть доступа к ним из сети Интернет блокируется. В принципе, экранирующий маршрутизатор может реализовать любую из политик безопасности, описанных ранее. Однако, если маршрутизатор не фильтрует пакеты по порту источника и номеру входного и выходного порта, реализация политики «запрещено все, что не разрешено в явной форме» может быть затруднена.

Схемы подключения межсетевых экранов с несколькими сетевыми интерфейсами. Схемы защиты с МЭ с одним сетевым интерфейсом недостаточно эффективны как с точки зрения безопасности, так и с позиций удобства конфигурирования. Они физически не разграничивают внутреннюю и внешнюю сети, а, соответственно, не могут обеспечивать надежную защиту межсетевых взаимодействий. Настройка таких межсетевых экранов, а также связанных с ними маршрутизаторов представляет собой довольно сложную задачу, цена решения которой превышает стоимость замены МЭ с одним сетевым интерфейсом на МЭ с двумя или тремя сетевыми интерфейсами. Поэтому далее будут более подробно рассмотрены схемы подключения межсетевых экранов с двумя и тремя сетевыми интерфейсами.

Защищаемую локальную сеть целесообразно представлять как совокупность закрытой и открытой подсетей. Здесь под *открытой подсетью* понимается подсеть, доступ к которой со стороны потенциально враждебной внешней сети может быть полностью или частично открыт. В открытую подсеть могут, например, входить общедоступные WWW-, FTP- и SMTP-серверы.

Среди множества возможных схем подключения МЭ типовыми являются следующие:

- схема единой защиты локальной сети;
- схема с защищаемой закрытой и незащищаемой открытой подсетями;
- схема с раздельной защитой закрытой и открытой подсетей.

Схема единой защиты локальной сети. Данная схема является наиболее простым решением (рис.9.5), котором МЭ целиком экранирует локальную сеть от потенциально враждебной внешней сети.

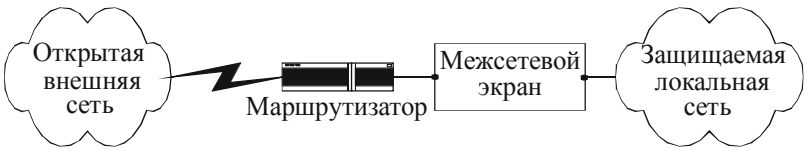

Рис.9.5. Схема единой защиты локальной сети

Между маршрутизатором и МЭ имеется только один путь, по которому идет весь трафик. Данный вариант МЭ реализует политику безопасности, основанную на принципе «запрещено все, что явно не разрешено», при этом пользователю недоступны все службы, кроме тех, для которых определены соответствующие полномочия. Обычно маршрутизатор настраивается таким образом, что МЭ является единственной видимой снаружи машиной.

Открытые серверы, входящие в локальную сеть, также будут защищены межсетевым экраном. Однако объединение серверов, доступных из внешней сети, вместе с другими ресурсами защищаемой локальной сети существенно снижает безопасность межсетевых взаимодействий. Поэтому данную схему подключения МЭ можно использовать лишь при отсутствии в локальной сети открытых серверов или когда имеющиеся открытые серверы делаются доступными из внешней сети только для ограниченного числа пользователей, которым можно доверять.

Поскольку межсетевой экран использует хост, то на нем могут быть установлены программы для усиленной аутентификации пользователей. Межсетевой экран может также протоколировать доступ, попытки зондирования и атак системы, что позволит выявить действия злоумышленников.

Для некоторых сетей может оказаться неприемлемой недостаточная гибкость схемы защиты на базе межсетевого экрана с двумя интерфейсами.

Схема с защищаемой закрытой и незащищаемой открытой подсетями. Если в составе локальной сети имеются общедоступные открытые серверы, тогда их целесообразно вынести как открытую подсеть до межсетевого экрана (рис.9.6).

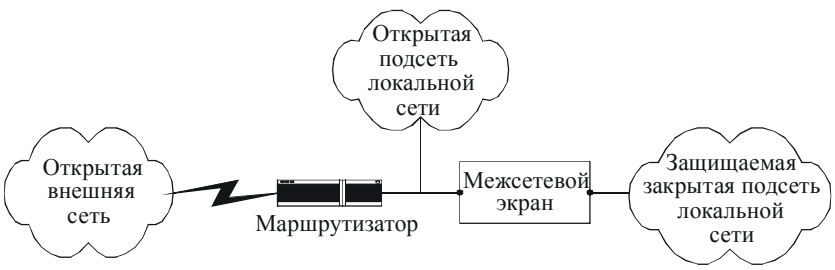

Рис.9.6. Схема с защищаемой закрытой и незащищаемой открытой подсетями

Данный способ обладает более высокой защищенностью закрытой части локальной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до межсетевого экрана.

Некоторые МЭ позволяют разместить эти серверы на себе. Однако такое решение не является лучшим с точки зрения безопасности самого МЭ и загрузки компьютера. Схему подключения МЭ с защищаемой закрытой подсетью и незащищаемой открытой подсетью целесообразно использовать лишь при невысоких требованиях по безопасности к открытой подсети.

Если же к безопасности открытых серверов предъявляются повышенные требования, тогда необходимо использовать схему с раздельной защитой закрытой и открытой подсетей [1, 3].

9.3.3. Персональные и распределенные сетевые экраны

За последние несколько лет в структуре корпоративных сетей произошли определенные изменения. Если раньше границы таких сетей можно было четко очертить, то сейчас это практически невозможно. Еще недавно такая граница проходила через все маршрутизаторы или иные устройства (например, модемы), через которые осуществлялся выход во внешние сети. В удаленных офисах организации ситуация была схожа. С появлением новых сервисов и технологий, в частности мобильного доступа к локальной вычислительной сети (ЛВС) или использования беспроводных сегментов сети, понятие «периметра» начинает терять свое значение.

Наиболее уязвимым местом корпоративной сети являются рабочие станции конечных пользователей, находящиеся за пределами защищаемого периметра, которые имеют, как правило, низкий уровень защиты. Все традиционные межсетевые экраны построены так, что защищаемые пользователи и ресурсы должны находиться под их защитой с внутренней стороны корпоративной или локальной сети, что является невозможным для мобильных пользователей.

Следует также упомянуть о такой проблеме, как обеспечение внутренней безопасности сети. Технология обеспечения внутренней безопасности отличается от технологии защиты периметра. Для отражения атак из внешней сети, по отношению к ЛВС, существуют весьма эффективные средства, которые помогают защитить рабочие станции пользователей от атак и других подозрительных действий, направленных на получение конфиденциальной информации. А вот отследить и предотвратить атаки, организуемые из локальной сети, по-прежнему достаточно сложно. И опасности, связанные с внутренней безопасностью, постоянно растут.

Для решения указанных проблем предложены следующие подходы: применение персональных и распределенных межсетевых экранов и использование возможностей виртуальных частных сетей VPN (Virtual Private Network), предлагаются такие технологии, как Total Access Protection (Check Point), Network Admission Control (Cisco), Network Access Protection (Microsoft), которые направлены на установление жесткого контроля защищенности конечных пользователей.

Для индивидуальных пользователей представляет интерес *технология персонального сетевого экранирования*. В этом случае сетевой экран устанавливается на защищаемый персональный компьютер. Такой экран, называемый персональным экраном компьютера (personal firewall) или системой сетевого экранирования, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко. Для защиты рабочего места пользователя кроме персонального МЭ необходимо иметь антивирус с актуальными сигнатурами, защиту доступа в корпоративную сеть через VPN.

В качестве примера персонального сетевого экрана можно указать межсетевой экран Windows Firewall, который служит первой линией защиты персонального компьютера от различного рода вредоносных программ. Начиная с версии Windows XP Service Pack 2 межсетевой экран Windows Firewall включен в ОС по умолчанию и защищает компьютер с момента загрузки операционной системы. Он удобен в использовании, легко настраивается, имеет простой интерфейс и практически незаметен при работе. В операционной системе Windows Vista межсетевой экран является двусторонним, позволяя осуществлять фильтрацию как входящего, так и исходящего трафика. Межсетевой экран Windows Firewall может блокировать весь входящий трафик до тех пор, пока на компьютер не будут установлены все последние пакеты обновлений.

При надлежащей настройке межсетевой экран Windows Firewall не позволяет большинству вредоносных программ проникать в систему, обеспечивая защиту от хакеров, вирусов и компьютерных «червей», которые пытаются получить доступ к компьютеру через Интернет.

Распределенный межсетевой экран представляет собой централизованно управляемую совокупность сетевых мини-экранов, защищающих отдельные компьютеры сети. При построении распределенных систем МЭ их функциональные компоненты распределяются по узлам сети и могут обладать различной функциональностью. При обнаружении подозрительных на атаку признаков управляющие модули распределенного МЭ могут адаптивно изменять конфигурацию, состав и расположение компонент.

Главное отличие распределенного межсетевого экрана от персонального экрана заключается в наличии у распределенного межсетевого экрана функции централизованного управления. Если персональные сетевые экраны управляются только с того компьютера, на котором они установлены, и идеально подходят для домашнего применения, то распределенные межсетевые экраны могут управляться централизованно, с единой консоли управления, установленной в главном офисе организации. Такие отличия позволили некоторым производителям выпускать свои решения МЭ в двух версиях:

- персональной (для индивидуальных пользователей);

- распределенной (для корпоративных пользователей).

Решения на основе распределенных или персональных межсетевых экранов наилучшим образом обеспечивают безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия.

9.3.4. Тенденции развития межсетевых экранов

Тенденции дальнейшего развития межсетевых экранов можно увидеть в некоторых продвинутых решениях современных МЭ. Неотъемлемыми свойствами современных корпоративных межсетевых экранов стали централизованное управление, инспекция разных сетевых и прикладных протоколов, поддержка NAT, интеграция с различными серверами аутентификации, фильтрация URL и т.д. Изменилась платформа, на которой реализуется межсетевой экран. Если раньше это было преимущественно программное решение, то постепенно произошел сдвиг в сторону аппаратной фильтрации трафика, что позволяет реализовать более скоростную и надежную обработку информационных потоков. Аппаратные межсетевые экраны могут быть выполнены в виде специальных модулей, интегрируемых в маршрутизаторы и коммутаторы.

Применение в межсетевых экранах технологии *deep packet inspection* позволяет проводить более глубокий анализ пропускаемого через МЭ трафика на предмет обнаружения различных нарушений и атак. Технология *deep packet inspection* позволяет вывести межсетевые экраны на качественно новый уровень и защитить приложения и сервисы, ранее считавшиеся незащищенными, например технологию IP-телефонии.

Важной тенденцией, влияющей на развитие межсетевых экранов, является их более тесная интеграция с другими решениями по информационной безопасности. Многофункциональное защитное устройство UTM (Unified Threat Management) обеспечивает высокий уровень защиты за счет тесной интеграции таких защитных технологий, как межсетевой экран, система предотвращения атак IPS, VPN, антивирус, антиспам, защита от шпионского ПО и т.п.

Вопросы для самоконтроля

1. Сформулируйте понятия «межсетевое экранирование» и «межсетевой экран» (firewall или брандмауэр).
2. Объясните суть фильтрации информационного потока межсетевым экраном.
3. Какие параметры могут использоваться в качестве критериев анализа информационного потока?
4. Какие варианты решений принимаются при интерпретации правил фильтрации информационного потока?
5. Что представляют собой функции посредничества МЭ и программы-посредники? Перечислите функции, которые могут выполнять программы-посредники.
6. Назовите дополнительные возможности МЭ. Объясните суть трансляции внутренних сетевых адресов для исходящих пакетов сообщений.
7. Опишите особенности функционирования экранирующего маршрутизатора (пакетного фильтра).
8. Опишите особенности функционирования межсетевых экранов экспертного уровня. Как выполняется фильтрация пакетов с контролем состояния соединения *(stateful inspection)*?
9. Укажите достоинства программно-аппаратного варианта исполнения межсетевых экранов.
10. Сформулируйте принципы формирования политики межсетевого взаимодействия, реализуемой системой МЭ.
11. Назовите основные схемы подключения межсетевых экранов. Опишите функционирование схемы с защищаемой закрытой и незащищаемой открытой подсетями.
12. Сформулируйте тенденции дальнейшего развития межсетевых экранов.

Глава 10. Виртуальные защищенные сети VPN

Никто не хранит тайны лучше
того, кто ее не знает.
Рохас Ф.

Современная инфраструктура корпораций включает в себя географически распределенные подразделения самой корпорации, ее партнеров, клиентов и поставщиков. В связи с бурным развитием Интернет и сетей коллективного доступа в мире произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные каналы связи. Предприятия стремятся использовать такие каналы для передачи критичной коммерческой и управленческой информации.

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования в бизнесе открытых сетей активно применяются виртуальные защищенные сети - VPN (Virtual Private Network).

10.1. Концепция построения виртуальных защищенных сетей VPN

В основе концепции построения виртуальных защищенных сетей VPN лежит достаточно простая идея: если в глобальной сети имеются два узла, которым нужно обменяться информацией, тогда между этими двумя узлами необходимо построить виртуальный защищенный туннель для обеспечения конфиденциальности и целостности информации, передаваемой через открытые сети. Доступ к этому виртуальному туннелю должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям.

Преимущества, получаемые компанией от создания таких виртуальных туннелей, заключаются прежде всего в значительной экономии финансовых средств, поскольку в этом случае компания может отказаться от построения или аренды дорогих выделенных каналов связи для создания собственных сетей Интранет/Экстранет и использовать для этого дешевые интернет-каналы.

10.1.1. Основные понятия и функции сети VPN

При подключении корпоративной локальной сети к открытой сети возникают угрозы безопасности двух типов:

- несанкционированный доступ к внутренним ресурсам корпоративной локальной сети;
- несанкционированный доступ к корпоративным данным в процессе их передачи по открытой сети.

Обеспечение безопасности информационного взаимодействия локальных сетей и отдельных компьютеров через открытые сети, в частности через сеть Интернет, возможно путем эффективного решения следующих задач:

- защита подключенных к открытым каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;
- защита информации в процессе ее передачи по открытым каналам связи.

Для защиты локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды обычно используют межсетевые экраны. Межсетевой экран располагают на стыке между локальной и открытой сетью. Для защиты отдельного удаленного компьютера, подключенного к открытой сети, на этом компьютере устанавливают программное обеспечение персонального сетевого экрана.

Защита информации в процессе ее передачи по открытым каналам основана на использовании виртуальных защищенных сетей VPN. *Виртуальной защищенной сетью VPN (Virtual Private Network)* называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

Виртуальная защищенная сеть VPN формируется путем построения виртуальных защищенных каналов связи, создаваемых на базе открытых каналов связи общедоступной сети. Эти виртуальные защищенные каналы связи называются *туннелями VPN*. Сеть VPN позволяет с помощью туннелей VPN соединить центральный офис, офисы филиалов, офисы бизнес-партнеров и удаленных пользователей и безопасно передавать информацию через Интернет (рис.10.1).

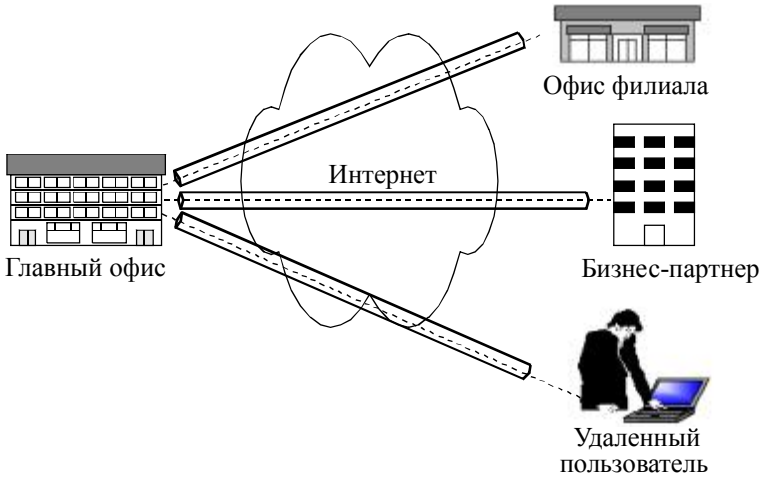

Рис.10.1. Виртуальная защищенная сеть VPN

Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети. Защита информации в процессе ее передачи по туннелю VPN основана на выполнении следующих функций:

- аутентификация взаимодействующих сторон;
- криптографическое закрытие (шифрование) передаваемых данных;
- проверка подлинности и целостности доставляемой информации.

При реализации этих функций используются криптографические методы защиты информации. Эффективность такой защиты обеспечивается за счет совместного использования симметричных и асимметричных криптографических систем. Туннель VPN, формируемый устройствами VPN, обладает свойствами защищенной выделенной линии, причем эта защищенная выделенная линия развертывается в рамках общедоступной сети, например Интернета. Устройства VPN могут играть в виртуальных частных сетях роль VPN-клиента, VPN-сервера или шлюза безопасности VPN.

VPN-клиент представляет собой программный или программно-аппаратный комплекс, выполняемый обычно на базе персонального компьютера. Его сетевое программное обеспечение модифицируется для выполнения шифрования и аутентификации трафика, которым это устройство обменивается с другими VPN-клиентами, VPN-серверами или шлюзами безопасности VPN. Обычно реализация VPN-клиента представляет собой программное решение, дополняющее стандартную операционную систему - Windows NT/2000/XP/Vista или Unix.

VPN-сервер представляет собой программный или программно-аппаратный комплекс, устанавливаемый на компьютере, выполняющем функции сервера. VPN-сервер обеспечивает защиту серверов от несанкционированного доступа из внешних сетей, а также организацию защищенных соединений (ассоциаций) с отдельными компьютерами и с компьютерами из сегментов локальных сетей, защищенных соответствующими VPN-продуктами. VPN-сервер является функциональным аналогом продукта VPN-клиент для серверных платформ. Он отличается прежде всего расширенными ресурсами для поддержания множественных соединений с VPN-клиентами. VPN-сервер может поддерживать защищенные соединения с мобильными пользователями.

Шлюз безопасности VPN (*security gateway*) - это сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов, расположенных за ним. Размещение шлюза безопасности VPN выполняется таким образом, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. Сетевое соединение шлюза VPN прозрачно для пользователей позади шлюза, оно представляется им выделенной линией, хотя на самом деле прокладывается через открытую сеть с коммутацией пакетов. Адрес шлюза безопасности VPN указывается как внешний адрес входящего туннелируемого пакета, а внутренний адрес пакета является адресом конкретного хоста позади шлюза. Шлюз безопасности VPN может быть реализован в виде отдельного программного решения, отдельного аппаратного устройства, а также в виде маршрутизатора или межсетевого экрана, дополненных функциями VPN.

Открытая внешняя среда передачи информации включает как каналы скоростной передачи данных, в качестве которой используется сеть Интернет, так и более медленные общедоступные каналы связи, в качестве которых могут применяться каналы телефонной сети. Эффективность виртуальной частной сети VPN определяется степенью защищенности информации, циркулирующей по открытым каналам связи.

Для безопасной передачи данных через открытые сети широко используют инкапсуляцию и туннелирование. С помощью методики туннелирования пакеты данных передаются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой «отправитель - получатель данных» устанавливается своеобразный туннель - логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

туннелирования состоит в том, чтобы инкапсулировать, т.е. «упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт». При этом пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Следует отметить, что туннелирование само по себе не защищает данные от несанкционированного доступа или искажения, но благодаря туннелированию появляется возможность полной криптографической защиты инкапсулируемых исходных пакетов. Чтобы обеспечить конфиденциальность передаваемых данных, отправитель шифрует исходные пакеты, упаковывает их во внешний пакет с новым IP-заголовком и отправляет по транзитной сети (рис.10.2).

Рис.10.2. Пример пакета, подготовленного для туннелирования

Особенностью туннелирования является то, что эта технология позволяет зашифровать исходный пакет целиком вместе с заголовком, а не только его поле данных. Это важно, поскольку некоторые поля заголовка содержат информацию, которая может быть использована злоумышленником. В частности, из заголовка исходного пакета можно извлечь сведения о внутренней структуре сети - данные о количестве подсетей и узлов и их IP-адресах. Злоумышленник может использовать такую информацию при организации атак на корпоративную сеть. Для защиты исходного пакета применяют его инкапсуляцию и туннелирование. Исходный пакет зашифровывают полностью вместе с заголовком и затем помещают в другой внешний пакет с открытым заголовком. Для транспортировки данных по открытой сети используются открытые поля заголовка внешнего пакета.

По прибытии в конечную точку защищенного канала из внешнего пакета извлекают внутренний исходный пакет, расшифровывают его и используют его восстановленный заголовок для дальнейшей передачи по внутренней сети (рис.10.3).

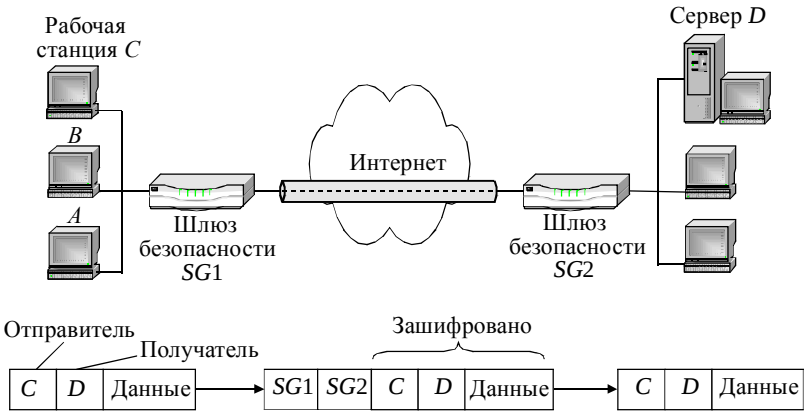

Рис.10.3. Схема виртуального защищенного туннеля

Туннелирование может быть использовано для защиты не только конфиденциальности содержимого пакета, но и его целостности и аутентичности, при этом электронную цифровую подпись можно распространить на все поля пакета.

В дополнение к сокрытию сетевой структуры между двумя точками туннелирование может также предотвратить возможный конфликт адресов между двумя локальными сетями. При создании локальной сети, не связанной с Интернет, компания может использовать любые IP-адреса для своих сетевых устройств и компьютеров. При объединении ранее изолированных сетей эти адреса могут начать конфликтовать друг с другом и с адресами, которые уже используются в Интернет. Инкапсуляция пакетов решает эту проблему, поскольку позволяет скрыть первоначальные адреса и добавить новые адреса, уникальные в пространстве IP-адресов Интернет, которые затем используются для пересылки данных по разделяемым сетям. Сюда же входит задача настройки IP-адреса и других параметров для мобильных пользователей, подключающихся к локальной сети.

Механизм туннелирования широко применяется для формирования защищенного канала. Обычно туннель создается только на участке открытой сети, где существует угроза нарушения конфиденциальности и целостности данных, например между точкой входа в открытый Интернет и точкой входа в

корпоративную сеть. При этом для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних исходных пакетах в защищенном виде. Туннелирование позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол. В результате появляется возможность решить проблемы взаимодействия нескольких разнотипных сетей.

Реализацию механизма туннелирования можно представить как результат работы протоколов трех типов: протокола-«пассажира», несущего протокола и протокола туннелирования. Например, в качестве протокола-«пассажира» может быть использован транспортный протокол IPX, переносящий данные в локальных сетях филиалов одного предприятия. Наиболее распространенным вариантом несущего протокола является протокол IP-сети Интернет. В качестве протокола туннелирования может быть использован протокол сетевого уровня IPSec. Туннели VPN могут создаваться для различных типов конечных пользователей - либо это локальная сеть LAN (local area network) с шлюзом безопасности, либо отдельные компьютеры удаленных и мобильных пользователей. Для создания виртуальной частной сети крупного предприятия нужны VPN-шлюзы, VPN-серверы и VPN-клиенты. VPN-шлюзы целесообразно использовать для защиты локальных сетей предприятия, VPN-серверы и VPN-клиенты используют для организации защищенных соединений удаленных и мобильных пользователей с корпоративной сетью через Интернет.

10.1.2. Варианты построения виртуальных защищенных каналов

Безопасность информационного обмена необходимо обеспечивать как в случае объединения локальных сетей, так и в случае доступа к локальным сетям удаленных или мобильных пользователей. При проектировании VPN обычно рассматриваются две основные схемы:

- виртуальный защищенный канал между локальными сетями (канал ЛВС - ЛВС);
- виртуальный защищенный канал между узлом и локальной сетью (канал клиент - ЛВС) (рис.10.4).

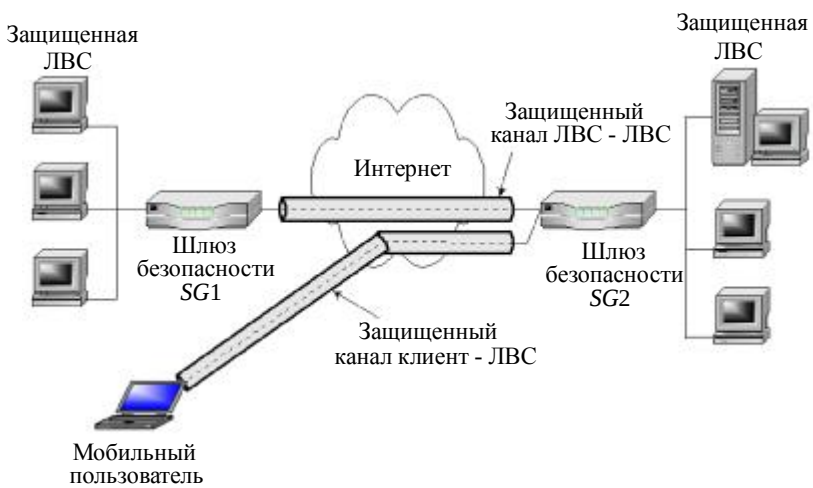

Рис.10.4. Виртуальные защищенные каналы типа ЛВС - ЛВС и клиент - ЛВС

Первая схема соединения позволяет создать постоянно доступные защищенные каналы между отдельными офисами. В этом случае шлюз безопасности служит интерфейсом между туннелем и локальной сетью и пользователи локальных сетей используют туннель для общения друг с другом.

Вторая схема защищенного канала VPN предназначена для установления соединений с удаленными или мобильными пользователями. Создание туннеля инициирует клиент (удаленный пользователь). Для связи со шлюзом, защищающим удаленную сеть, он запускает на своем компьютере специальное клиентское программное обеспечение. Этот вид VPN заменяет собой коммутируемые соединения и может использоваться наряду с традиционными методами удаленного доступа.

Существует ряд вариантов схем виртуальных защищенных каналов. В принципе, любой из двух узлов виртуальной корпоративной сети, между которыми формируется виртуальный защищенный канал, может принадлежать конечной или промежуточной точке защищаемого потока сообщений.

С точки зрения обеспечения информационной безопасности лучшим является вариант, при котором конечные точки защищенного туннеля совпадают с конечными точками защищаемого потока сообщений. В этом случае обеспечивается защищенность канала вдоль всего пути следования пакетов сообщений. Однако такой вариант ведет к децентрализации управления и избыточности ресурсных затрат. В этом случае необходима установка средств создания VPN на каждом клиентском компьютере локальной сети.

Если внутри локальной сети, входящей в виртуальную сеть, не требуется защита трафика, тогда в качестве конечной точки защищенного туннеля можно выбрать межсетевой экран или пограничный маршрутизатор этой локальной сети. Если же поток сообщений внутри локальной сети должен быть защищен, тогда в качестве конечной точки туннеля в этой сети должен выступать компьютер, который участвует в защищенном взаимодействии. При доступе к локальной сети удаленного пользователя компьютер этого пользователя должен быть конечной точкой виртуального защищенного канала.

Защищенный туннель создается компонентами виртуальной сети, функционирующими на узлах, между которыми формируется туннель. Эти компоненты принято называть инициатором туннеля и терминатором туннеля.

Инициатор туннеля инкапсулирует исходный пакет в новый пакет, содержащий новый заголовок с информацией об отправителе и получателе. Все передаваемые по туннелю пакеты являются пакетами IP. Маршрут между инициатором и терминатором туннеля определяет обычная маршрутизируемая сеть IP, которая может быть сетью, отличной от Интернет.

Инициировать и разрывать туннель могут различные сетевые устройства и программное обеспечение. Например, туннель может быть инициирован ноутбуком мобильного пользователя, оборудованным модемом и соответствующим программным обеспечением для установления соединений удаленного доступа. В качестве инициатора может выступить также маршрутизатор локальной сети, наделенный соответствующими функциональными возможностями. Туннель обычно завершается коммутатором сети или шлюзом провайдера услуг.

Терминатор туннеля выполняет процесс, обратный инкапсуляции. Терминатор удаляет новые заголовки и направляет каждый исходный пакет адресату в локальной сети.

Конфиденциальность инкапсулируемых пакетов обеспечивается путем их шифрования, а целостность и подлинность - путем формирования электронной цифровой подписи. Существует множество методов и алгоритмов криптографической защиты данных, поэтому необходимо, чтобы инициатор и терминатор туннеля своевременно согласовали друг с другом и использовали одни и те же методы и алгоритмы защиты. Для обеспечения возможности расшифрования данных и проверки цифровой подписи при приеме инициатор и терминатор туннеля должны также поддерживать функции безопасного обмена ключами. Кроме того, конечные стороны информационного взаимодействия должны пройти аутентификацию, чтобы гарантировать создание туннелей VPN только между уполномоченными пользователями.

Существующая сетевая инфраструктура корпорации может быть подготовлена к использованию VPN как с помощью программного, так и с помощью аппаратного обеспечения.

10.1.3. Методы обеспечения безопасности VPN

При построении защищенной виртуальной сети VPN первостепенное значение имеет задача обеспечения информационной безопасности. Под безопасностью данных понимают их конфиденциальность, целостность и доступность. Применительно к задачам VPN критерии безопасности данных могут быть определены следующим образом:

- *конфиденциальность* - гарантия того, что в процессе передачи данных по защищенным каналам VPN эти данные могут быть известны только легальным отправителю и получателю;
- *целостность* - гарантия сохранности передаваемых данных во время прохождения по защищенному каналу VPN;
- *доступность* - гарантия того, что средства, выполняющие функции VPN, постоянно доступны легальным пользователям.

Конфиденциальность обеспечивается с помощью различных методов и алгоритмов симметричного и асимметричного шифрования. Целостность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на асимметричных методах шифрования и односторонних функциях.

Аутентификация осуществляется на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт, протоколов строгой аутентификации и обеспечивает установление VPN-соединения только между легальными пользователями и предотвращает доступ к средствам VPN нежелательных лиц.

Авторизация подразумевает предоставление абонентам, доказавшим свою легальность (аутентичность), разных видов обслуживания, в частности разных способов шифрования их трафика. Авторизация и управление доступом часто реализуются одними и теми же средствами.

Для обеспечения безопасности передаваемых данных в виртуальных защищенных сетях должны быть решены следующие основные задачи безопасности:

- взаимная аутентификация абонентов при установлении соединения;
- обеспечение конфиденциальности, целостности и аутентичности передаваемой информации;
- авторизация и управление доступом.

10.2. VPN-решения для построения защищенных сетей

В настоящее время технологии виртуальных защищенных частных сетей (VPN) привлекают внимание как средних, так и крупных компаний (банков, ведомств, крупных государственных структур и т.д.). Это обусловлено тем, что VPN-технологии позволяют компаниям не только существенно сократить свои расходы на содержание выделенных каналов связи с удаленными подразделениями (филиалами), но и повысить конфиденциальность обмена информацией.

VPN-технологии позволяют организовывать защищенные туннели как между офисами компании, так и к отдельным рабочим станциям и серверам. При этом неважно, через какого провайдера Интернет конкретная рабочая станция подключится к защищенным ресурсам предприятия. Все что увидит сторонний наблюдатель - поток IP-пакетов с нераспознаваемым содержимым [1, 11].

Рынок VPN-продуктов предлагает потенциальным клиентам широкий спектр оборудования и ПО для создания виртуальных защищенных сетей: от интегрированных многофункциональных и специализированных устройств до чисто программных продуктов.

10.2.1. Классификация сетей VPN по рабочему уровню модели OSI

Благодаря преимуществам технологии VPN многие компании строят свою стратегию с учетом использования Интернета в качестве главного средства передачи информации, причем даже той, которая является уязвимой или жизненно важной.

Для технологий безопасной передачи данных по общедоступной (незащищенной) сети применяют обобщенное название - *защищенный канал (secure channel).* Термин «канал» подчеркивает тот факт, что защита данных обеспечивается между двумя узлами сети (хостами или шлюзами) вдоль некоторого виртуального пути, проложенного в сети с коммутацией пакетов.

Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях модели взаимодействия открытых систем OSI (Open Systems Interconnection) (рис.10.5) [1].

<table>
<tr><td rowspan="8">Протоколы защищенного доступа</td><td>ПРИКЛАДНОЙ</td><td rowspan="3">Влияют на приложения</td></tr>
<tr><td>ПРЕДСТАВИТЕЛЬНЫЙ</td></tr>
<tr><td>СЕАНСОВЫЙ</td></tr>
<tr><td>ТРАНСПОРТНЫЙ</td><td></td></tr>
<tr><td>СЕТЕВОЙ</td><td rowspan="3">Прозрачны для приложений</td></tr>
<tr><td>КАНАЛЬНЫЙ</td></tr>
<tr><td>ФИЗИЧЕСКИЙ</td></tr>
</table>

Рис.10.5. Уровни протоколов защищенного канала

Класификация VPN по рабочему уровню модели OSI представляет значительный интерес, поскольку от выбранного уровня OSI во многом зависит функциональность реализуемой VPN и ее совместимость с приложениями корпоративной информационной системы, а также с другими средствами защиты.

По признаку «рабочий уровень» модели OSI различают следующие группы VPN:

- канального уровня;
- сетевого уровня;
- сеансового уровня [1, 3] .

Нетрудно заметить, что VPN строятся на достаточно низких уровнях модели OSI. Причина этого достаточно проста - чем ниже в стеке реализованы средства защищенного канала, тем проще их сделать прозрачными для приложений и прикладных протоколов. На сетевом и канальном уровнях зависимость приложений от протоколов защиты исчезает совсем. Поэтому построить универсальную и прозрачную защиту для пользователя возможно только на нижних уровнях модели. Однако здесь возникает другая проблема - зависимость протокола защиты от конкретной сетевой технологии.

Если для защиты данных используется протокол одного из верхних уровней (прикладного или представительного), то такой способ защиты не зависит от того, какие сети (IP или IPX, Ethernet или ATM) применяются для транспортировки данных, что можно считать несомненным достоинством. Однако приложение при этом становится зависимым от конкретного протокола защиты, т.е. для приложений такой протокол не является прозрачным.

Защищенному каналу на самом высоком, прикладном уровне свойственен еще один недостаток - ограниченная область действия. Протокол защищает только вполне определенную сетевую службу - файловую, гипертекстовую или почтовую. Например, протокол S/MIME защищает исключительно сообщения электронной почты. Поэтому для каждой службы необходимо разрабатывать соответствующую

защищенную версию протокола. Следует отметить, что на верхних уровнях модели OSI существует достаточно жесткая связь между используемым стеком протоколов и приложением.

Рассмотрим более подробно группы VPN, работающие на канальном, сетевом и сеансовом уровнях модели OSI.

VPN канального уровня. Средства VPN, используемые на канальном уровне модели OSI, позволяют обеспечить инкапсуляцию различных видов трафика третьего уровня (и более высоких уровней) и построение виртуальных туннелей типа точка-точка (от маршрутизатора к маршрутизатору или от персонального компьютера к шлюзу ЛВС). К этой группе относятся VPN-продукты, которые используют протоколы L2F (Layer 2 Forwarding) и PPTP (Point-to-Point Tunneling Protocol), а также стандарт L2TP (Layer 2 Tunneling Protocol), разработанный совместно фирмами Cisco Systems и Microsoft [1].

Протокол защищенного канала PPTP основан на протоколе PPP, который широко используется в соединениях точка-точка, например при работе по выделенным линиям. Протокол PPTP обеспечивает прозрачность средств защиты для приложений и служб прикладного уровня и не зависит от применяемого протокола сетевого уровня. В частности, протокол PPTP может переносить пакеты как в сетях IP, так и в сетях, работающих на основе протоколов IPX, DECnet или NetBEUI. Однако, поскольку протокол PPP используется далеко не во всех сетях (в большинстве локальных сетей на канальном уровне работает протокол Ethernet, а в глобальных - протоколы ATM, frame relay), PPTP нельзя считать универсальным средством. В разных частях крупной составной сети, вообще говоря, используются разные канальные протоколы, поэтому проложить защищенный канал через эту гетерогенную среду с помощью единого протокола канального уровня невозможно.

VPN сетевого уровня. VPN-продукты сетевого уровня выполняют инкапсуляцию IP в IP. Одним из широко известных протоколов на этом уровне является протокол IPSec (IP Security), предназначенный для аутентификации, туннелирования и шифрования IP-пакетов. Стандартизованный консорциумом Internet Engineering Task Force (IETF) протокол IPSec вобрал в себя все лучшие решения по шифрованию пакетов [1, 11].

Работающий на сетевом уровне протокол IPSec является компромиссным вариантом. С одной стороны, он прозрачен для приложений, а с другой - может работать практически во всех сетях, так как основан на широко распространенном протоколе IP. Протокол IPSec предусматривает стандартные методы идентификации пользователей или компьютеров при инициации туннеля, стандартные способы использования шифрования конечными точками туннеля, а также стандартные методы обмена и управления ключами шифрования между конечными точками.

Протокол IPSec является доминирующим методом VPN для взаимодействия ЛВС. Протокол IPSec может работать совместно с протоколом L2TP, в результате эти два протокола обеспечивают надежную идентификацию, стандартизованное шифрование и целостность данных. Туннель IPSec между двумя локальными сетями может поддерживать множество индивидуальных каналов передачи данных, в результате чего приложения данного типа получают преимущества с точки зрения масштабирования по сравнению с технологией второго уровня.

С протоколом IPSec связан протокол IKE (Internet Key Exchange), решающий задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами. Протокол IKE автоматизирует обмен ключами и устанавливает защищенное соединение, тогда как IPSec кодирует и «подписывает» пакеты. Кроме того, IKE позволяет изменять ключ для уже установленного соединения, что повышает конфиденциальность передаваемой информации.

VPN сеансового уровня. Некоторые VPN используют другой подход под названием «посредники каналов» (circuit proxy). Этот метод функционирует над транспортным уровнем и ретранслирует трафик из защищенной сети в общедоступную сеть Интернет для каждого сокета в отдельности. (Сокет IP идентифицируется комбинацией TCP-соединения и конкретного порта или заданным портом UDP. Стек TCP/IP не имеет пятого - сеансового - уровня, однако ориентированные на сокеты операции часто называют операциями сеансового уровня.)

Шифрование информации, передаваемой между инициатором и терминатором туннеля, часто осуществляется с помощью защиты транспортного уровня TLS (Transport Layer Security). Для стандартизации аутентифицированного прохода через межсетевые экраны консорциум IETF определил протокол под названием SOCKS, и в настоящее время протокол SOCKS v.5 применяется для стандартизованной реализации посредников каналов [1, 11].

Если протокол IPSec, по существу, распространяет сеть IP на защищенный туннель, то продукты на базе протокола SOCKS расширяют ее на каждое приложение и каждый сокет в отдельности. В отличие от решений уровня 3 (и уровня 2), где созданные туннели 2 и 3 уровня функционируют одинаково в обоих направлениях, сети VPN уровня 5 допускают независимое управление передачей в каждом направлении. Аналогично протоколу IPSec и протоколам второго уровня сети VPN уровня 5 можно использовать с другими типами виртуальных частных сетей, поскольку данные технологии не являются взаимоисключающими.

10.2.2. Основные варианты архитектуры VPN

Существует множество разновидностей виртуальных частных сетей. Их спектр варьируется от провайдерских сетей, позволяющих управлять обслуживанием клиентов непосредственно на их площадях,

до корпоративных сетей VPN, разворачиваемых и управляемых самими компаниями. Тем не менее, принято выделять по архитектуре технического решения три основных вида виртуальных частных сетей:

- VPN с удаленным доступом (Remote Access VPN);
- внутрикорпоративные VPN (Intranet VPN);
- межкорпоративные VPN (Extranet VPN).

VPN с удаленным доступом. Виртуальные частные сети VPN с удаленным доступом (Remote Access VPN) обеспечивают защищенный удаленный доступ к информационным ресурсам предприятия для мобильных или удаленных сотрудников корпорации (руководство компанией, сотрудники, находящиеся в командировках, сотрудники-надомники и т.д.).

Виртуальные частные сети с удаленным доступом (рис.10.6)

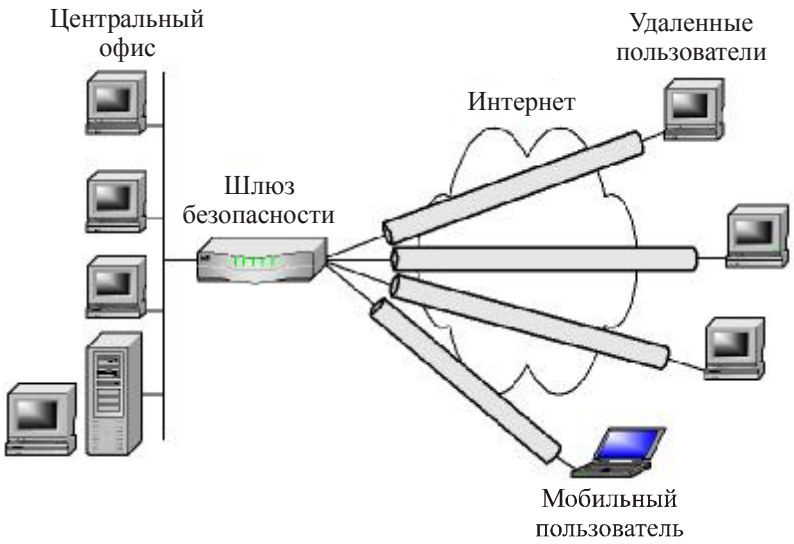

Рис.10.6. Виртуальная частная сеть с удаленным доступом

завоевали всеобщее признание благодаря тому, что они позволяют значительно сократить ежемесячные расходы на использование коммутируемых и выделенных линий. Принцип их работы прост: пользователи устанавливают соединения с местной точкой доступа к глобальной сети, после чего их вызовы туннелируются через Интернет, что позволяет избежать платы за междугородную и международную связь или выставления счетов владельцам бесплатных междугородных номеров. Затем все вызовы концентрируются на соответствующих узлах и передаются в корпоративные сети.

Применение Remote Access VPN обеспечивает ряд преимуществ, в частности:

- эффективная система установления подлинности удаленных и мобильных пользователей, которая обеспечивается надежной процедурой аутентификации;
- высокая масштабируемость и простота развертывания для новых пользователей, добавляемых к сети;
- сосредоточение внимания компании на основных корпоративных бизнес-целях вместо отвлечения на проблемы обеспечения работы сети.

Существенная экономия при использовании Remote Access VPN является мощным стимулом, однако применение открытого Интернет в качестве объединяющей магистрали для транспорта чувствительного корпоративного трафика становится все более масштабным, что делает механизмы защиты информации жизненно важными элементами данной технологии.

Внутрикорпоративная сеть VPN. Внутрикорпоративные сети VPN (Интранет VPN) используются для организации защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными сетями связи. Компании, нуждающиеся в организации доступа к централизованным хранилищам информации для своих филиалов и отделений, могут соединить удаленные узлы при помощи виртуальной частной сети (рис.10.7).

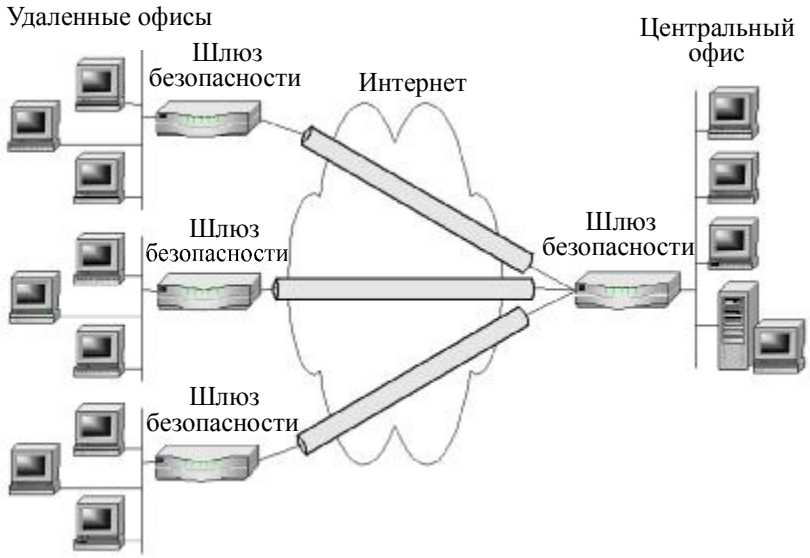

Рис.10.7. Соединение узлов сети с помощью технологии Интранет VPN

Сети Интранет VPN строятся с использованием Интернет или разделяемых сетевых инфраструктур, предоставляемых сервис-провайдерами. Компания может отказаться от использования дорогостоящих выделенных линий, заменив их более дешевой связью через Интернет.

Для Интранет VPN характерны следующие достоинства:

- применение мощных криптографических протоколов шифрования данных для защиты конфиденциальной информации;
- надежность функционирования при выполнении таких критических приложений, как системы автоматизированной продажи и системы управления базами данных;
- гибкость управления для более эффективного размещения быстро возрастающего количества новых пользователей, новых офисов и новых программных приложений.

Построение Интранет VPN, использующее Интернет, является самым рентабельным способом реализации VPN-технологии.

Межкорпоративная сеть VPN. Межкорпоративные сети VPN (Экстранет VPN) используются для организации эффективного взаимодействия и защищенного обмена информацией со стратегическими партнерами по бизнесу, в том числе зарубежными, основными поставщиками, крупными заказчиками, клиентами и т.д. (рис.10.8).

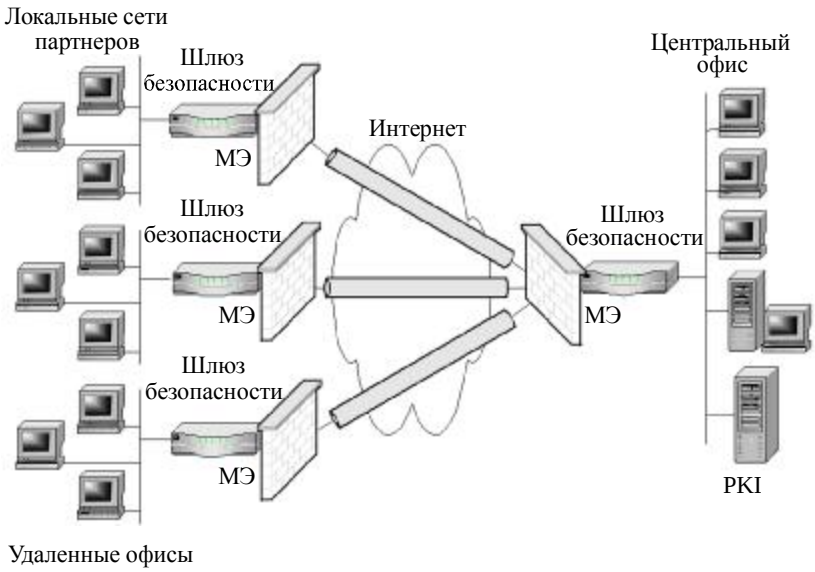

Рис.10.8. Межкорпоративная сеть Экстранет VPN

Экстранет - это сетевая технология, которая обеспечивает прямой доступ из сети одной компании к сети другой компании и, таким образом, способствует повышению надежности связи, поддерживаемой в ходе делового сотрудничества.

Сети Экстранет VPN в целом похожи на внутрикорпоративные виртуальные частные сети с той лишь разницей, что проблема защиты информации является для них более острой. Для Экстранет VPN характерно

использование стандартизированных VPN-продуктов, гарантирующих способность к взаимодействию с различными VPN-решениями, которые деловые партнеры могли бы применять в своих сетях.

Когда несколько компаний принимают решение работать вместе и открывают друг для друга свои сети, они должны позаботиться о том, чтобы их новые партнеры имели доступ только к определенной информации. При этом конфиденциальная информация должна быть надежно защищена от несанкционированного использования. Именно поэтому в межкорпоративных сетях большое значение придается контролю доступа из открытой сети посредством межсетевых экранов. Важна и аутентификация пользователей, призванная гарантировать, что доступ к информации получают только те, кому он действительно разрешен. Вместе с тем, развернутая система защиты от несанкционированного доступа не должна привлекать к себе внимания.

Соединения Экстранет VPN развертываются, используя те же самые архитектуру и протоколы, которые применяются при реализации Интранет VPN и Remote Access VPN. Основное различие заключается в том, что разрешение доступа, которое дается пользователям Экстранет VPN, связано с сетью их партнера.

Иногда в отдельную группу выделяют локальный вариант сети VPN (Localnet VPN). Локальная сеть Localnet VPN обеспечивает защиту информационных потоков, циркулирующих внутри локальных сетей компании (как правило, Центрального офиса), от несанкционированного доступа со стороны «излишне любопытных» сотрудников самой компании. В настоящее время наблюдается тенденция к конвергенции различных способов реализаций VPN [1].

10.2.3. Виды технической реализации VPN

Средства построения виртуальных защищенных сетей VPN отличаются большим разнообразием. По способу технической реализации различают группы VPN на основе:

- маршрутизаторов;
- межсетевых экранов;
- программных решений;
- специализированных аппаратных средств.

Каждое из перечисленных решений имеет свои достоинства и недостатки. Следует иметь в виду, что корпоративные заказчики предъявляют, как правило, достаточно жесткие требования к таким характеристикам VPN, как:

- интегрируемость с уже существующими в подразделениях компании средствами защиты информации, а также прозрачность работы VPN для всех работающих внутрикорпоративных приложений (системы документооборота, системы аудита и управления компьютерными сетями и т.д.);
- масштабируемость применяемых технических решений;
- пропускная способность защищаемой сети, т.е. VPN устройства не должны вносить существенные задержки в процесс обработки и передачи информации, а также заметно суживать полосу пропускания канала связи;
- стойкость применяемых криптоалгоритмов, а также обеспечение целостности передаваемой по сетям информации и надежной аутентификации пользователей VPN;
- унифицируемость VPN решения, позволяющая данной компании в будущем без особых технических и организационных проблем устанавливать защищенные соединения с новыми партнерами по бизнесу;
- общая совокупная стоимость построения корпоративной VPN.

VPN на основе маршрутизаторов. Маршрутизатор пропускает через себя все пакеты, которыми локальная сеть обменивается с внешним миром. Это делает маршрутизатор естественной платформой для шифрования исходящих пакетов и расшифрования криптозащищенных входящих пакетов. Иными словами, маршрутизатор может, в принципе, совмещать основные операции по маршрутизации с поддержанием функций VPN.

Такое решение имеет свои достоинства и недостатки. Достоинства заключаются в удобстве совместного администрирования функций маршрутизации и функций VPN. Использование маршрутизаторов для поддержания VPN особенно полезно в тех случаях, когда предприятие не использует межсетевой экран и организует защиту корпоративной сети только с помощью маршрутизатора, совмещающего функции защиты как по доступу в сеть, так и по шифрованию передаваемого трафика. Недостатки данного решения связаны с повышенными требованиями к производительности маршрутизатора, вынужденного совмещать основные операции по маршрутизации с трудоемкими операциями шифрования и аутентификации трафика.

Проблема получения повышенной производительности маршрутизатора обычно решается с помощью аппаратной поддержки функций шифрования. Сегодня практически все ведущие производители маршрутизаторов и других сетевых устройств заявляют о поддержке в своих продуктах различных VPN-протоколов.

VPN на основе межсетевых экранов. Через межсетевой экран локальной сети, как и через маршрутизатор, пропускается весь трафик. Поэтому функции зашифрования исходящего трафика и расшифрования входящего трафика может с успехом выполнять и МЭ. Сегодня ряд VPN-решений

опирается на расширения МЭ дополнительными функциями поддержки VPN, что позволяет установить через Интернет шифрованное соединение с другим МЭ.

Построение VPN на базе межсетевых экранов является вполне обоснованным решением с точки зрения обеспечения комплексной защиты корпоративной сети от атак из открытых сетей. Действительно, при объединении функций МЭ и VPN-шлюза в одной точке под контролем единой системы управления и аудита все функции по защите корпоративной сети оказываются сосредоточенными в одном устройстве, при этом повышается качество администрирования средств защиты.

Однако такая универсализация средства защиты при существующем уровне возможностей вычислительных средств имеет не только положительные, но и отрицательные стороны. Вычислительная сложность у операций шифрования и аутентификации намного выше, чем у традиционных для межсетевого экрана операций фильтрации пакетов. Поэтому МЭ, рассчитанный на выполнение менее трудоемких операций, часто не обеспечивает нужную производительность при выполнении дополнительных функций VPN. Когда корпоративная сеть подключена к открытой сети высокоскоростным каналом, рекомендуется для обеспечения качественной защиты использовать VPN-шлюз, выполненный в виде отдельного аппаратного, программного или комбинированного устройства.

Ряд производителей МЭ расширяют поддержку функций VPN в своих продуктах. Ведущими производителями межсетевых экранов с поддержкой функций VPN являются компании Check Point Software Technologies, Network Associates, Secure Computing и др. В частности, компания Check Point Software Technologies, чей межсетевой экран FireWall-1 многократно признавался лучшим, выпускает популярное семейство продуктов VPN-1, которое тесно интегрировано с FireWall-1.

Большинство МЭ представляет собой серверное программное обеспечение, поэтому актуальная проблема повышения производительности может быть решена за счет применения высокопроизводительной компьютерной платформы. Построение VPN на базе МЭ выглядит вполне рациональным решением, хотя ему присущи некоторые недостатки. Прежде всего это высокая стоимость данного решения в пересчете на одно рабочее место корпоративной сети и достаточно высокие требования к производительности МЭ даже при умеренной ширине полосы пропускания выходного канала связи.

VPN на основе специализированного программного обеспечения. Для построения VPN широко используются специализированные программные средства. Программные средства построения VPN позволяют формировать защищенные туннели чисто программным образом и превращают компьютер, на котором они функционируют, в маршрутизатор, который получает зашифрованные пакеты, расшифровывает их и передает по локальной сети дальше, к конечной точке назначения. В последнее время появилось достаточно много таких продуктов. В виде специализированного программного обеспечения могут быть выполнены VPN-шлюзы, VPN-серверы и VPN-клиенты.

VPN-продукты, реализованные программным способом, с точки зрения производительности уступают специализированным аппаратным устройствам, в то же время программные продукты легко обеспечивают производительность, достаточную для удаленного доступа. Несомненным достоинством программных продуктов является гибкость и удобство в применении, а также относительно невысокая стоимость. Многие компании-производители аппаратных шлюзов дополняют линейку своих продуктов чисто программной реализацией VPN-клиента, который рассчитан на работу в среде стандартной ОС.

VPN на основе специализированных аппаратных средств. Главным преимуществом VPN-средств на основе специализированных аппаратных устройств является их высокая производительность. Объем вычислений, которые необходимо выполнить при обработке VPN-пакета, в 50 - 100 раз превышает тот, который требуется для обработки обычного пакета. Более высокое быстродействие VPN-систем на базе аппаратных средств достигается благодаря тому, что шифрование в них осуществляется специализированными микросхемами.

Такие VPN-средства применяются для формирования криптозащищенных туннелей между локальными сетями. Оборудование для формирования VPN от некоторых производителей одновременно поддерживает и защищенную связь в режиме «удаленный компьютер - локальная сеть».

Аппаратные VPN-шлюзы реализуются в виде отдельного аппаратного устройства, основной функцией которого является высокопроизводительное шифрование трафика. Эти VPN-шлюзы работают с цифровыми сертификатами X.509 и инфраструктурой управления открытыми ключами PKI, поддерживают работу со справочными службами по LDAP.

Специализированные аппаратные VPN-средства лидируют практически по всем возможным показателям, кроме стоимости. Специализированное аппаратное VPN-оборудование является предпочтительным решением для ответственных применений.

10.3. Современные VPN-продукты

Продукты сетевой безопасности выпускают в настоящее время ряд российских компаний: ЛАН Крипто, ООО фирма «Анкад», компания «С-Терра СиЭсПи», НИП «Информзащита», ОАО «ИнфоТеКС», ООО «Фактор-ТС» и др.

Сравнительный анализ продуктов сетевой безопасности российских производителей показал, что новая версия семейства VPN-продуктов CSP VPN 3.0 компании «С-Терра СиЭсПи» имеет высокие характеристики, отличающиеся оптимизированной производительностью и повышенной устойчивостью при их функционировании на многопроцессорных (многоядерных) платформах [25]. Рассмотрим семейство VPN-продуктов CSP VPN.

CSP VPN-агенты российской компании «С-Терра СиЭсПи» являются частью решения по безопасности Cisco, адаптированного к российским стандартам информационной безопасности, и предназначены для использования в рамках идеологии CiscoSAFE. Реализована совместимость продуктов семейства CSP VPN Gate с системой централизованного управления Cisco Security Manager (CS Manager). Эта система обеспечивает централизованное управление политиками безопасности МЭ, VPN и IPS, масштабируемость, наследование политик, группирование устройств и визуальное управление политиками, ролевой механизм управления правами доступа и документооборот по операциям. В результате пользователи получают гибкий, надежный, прозрачный и эффективный инструмент централизованного управления всеми устройствами сети, включая продукты CSP VPN Gate.

Среди других нововведений и улучшений можно отметить поддержку операционных систем Windows Vista.

Функционально полный комплект средств сетевой защиты CSP VPN обеспечивает:

- защиту индивидуальных пользователей;
- защиту серверов;
- защиту отдельных сетей;
- защиту специализированных устройств.

Продуктная линия CSP VPN включает:

- *CSP VPN Client* - программный продукт для защиты индивидуальных пользователей;
- *CSP VPN Server* - программный продукт для сетевой защиты серверов;
- *CSP VPN Gate 100B* - программно-аппаратный комплекс - шлюз безопасности, ориентированный на защиту специализированных устройств;
- *CSP VPN Gate 100* - программно-аппаратный комплекс - шлюз безопасности, ориентированный на защиту малых офисов (до 10 компьютеров);
- *CSP VPN Gate 1000* - программно-аппаратный комплекс - шлюз безопасности, ориентированный на защиту малых офисов (до 50 компьютеров);
- *CSP VPN Gate 3000* - программно-аппаратный комплекс - шлюз безопасности, ориентированный на защиту средних офисов (до 250 компьютеров);
- *CSP VPN Gate 7000* - программно-аппаратный комплекс - шлюз безопасности, ориентированный на защиту крупных офисов (свыше 250 компьютеров);
- *модуль NME-RVPN (Russia VPN Network Module)* - программно-аппаратный комплекс - шлюз безопасности, предназначенный для использования в составе маршрутизаторов серии Cisco® 2800 и 3800 Integrated Services Routers.

Модуль NME-RVPN. Модуль NME-RVPN (рис.10.9)

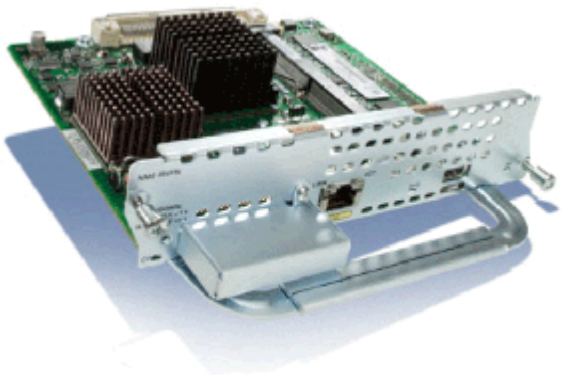

Рис.10.9. Модуль NME-RVPN

в составе маршрутизаторов серии Cisco® 2800 и 3800 Integrated Services Routers предлагает российским потребителям уникальное устройство, позволяющее обеспечить как эффективную маршрутизацию, так и защиту трафика данных, голоса, видео. При этом устройство управляется как единое целое, используя интерфейс Cisco для формирования правил маршрутизации и защиты сетевых взаимодействий. Подобная глубокая интеграция позволяет существенно уменьшить сложность сети, не предъявлять дополнительных требований к квалификации персонала и, как результат, снизить затраты на развертывание и поддержку, а также сроки развертывания подсистемы информационной безопасности.

Обеспечение защищенности сетевых взаимодействий. В связи с широкой интеграцией корпоративных коммуникаций с публичными сетями для обеспечения взаимодействий компаний с

филиалами, удаленными пользователями, заказчиками и партнерами первостепенное значение приобретает вопрос обеспечения российских пользователей высокотехнологичным сертифицированным VPN-решением в сочетании с передовыми технологиями Cisco Systems и удовлетворяющим современным требованиям эффективной защиты всех видов сетевых взаимодействий. При этом необходимо не только решить вопросы защиты внешнего обмена данными, но и предоставить современные решения по защищенным беспроводным коммуникациям, защите голоса и видео с обеспечением качества обслуживания, максимально эффективно защитить взаимодействие клиентов в сетях операторов связи и услуг.

Интеграция модуля NME-RVPN в маршрутизаторы серии Cisco 2800 или 3800 Integrated Services Router позволяет потребителям получить единое решение, обеспечивающее организацию сетевой защиты, использующей российскую сертифицированную криптографию, развитую маршрутизацию, качество обслуживания приоритетного трафика (QoS), сервисы IP-телефонии и видео, коммутацию сетей. Подобные качества совместно с управляемостью и технологий Cisco IOS практически полностью закрывают потребность современного бизнеса в организации и защите ответственных, критически важных сетевых взаимодействий.

Программное обеспечение CSP VPN Gate. Программное обеспечение CSP VPN Gate, входящее в состав модуля NME-RVPN, является еще одним элементом семейства продуктов CSP VPN Client, CSP VPN Server и масштабируемой серии шлюзов безопасности CSP VPN Gate 100/1000/3000/7000/10000.

Продукты CSP VPN обеспечивают базовую функциональность современного VPN-устройства:

- шифрование (конфиденциальность) и ЭЦП (целостность, аутентификация) IP-пакетов, целостность потока пакетов;
- маскировку топологии сети за счет инкапсуляции трафика в защищенный туннель;
- прозрачность для NAT (поддержка инкапсуляции пакета ESP в UDP);
- аутентификацию узлов сети и пользователей, контроль доступа на уровне компьютеров, пользователей и приложений, интегрированный межсетевой экран 4-го класса (CSP VPN Gate удовлетворяет требованиям к межсетевому экрану по 4-му классу защищенности);
- обеспечение надежности с выравниванием нагрузки в схеме резервирования N + 1 (Dead Peer Detection protocol);
- унификацию политики безопасности для мобильных и «внутренних» пользователей (динамическое конфигурирование корпоративных IP-адресов для удаленных пользователей «внутри VPN»);
- сохранение классификации трафика для защищенных пакетов, приоритетную обработку трафика голоса и видео (поддержка QoS), отсутствие потери пакетов при регенерации сессионных ключей (smooth IKE re-keying);
- гибкое, централизованное и событийное ведение журнала с возможностью вторичной обработки на основе протокола Syslog.

Как результат, применение модуля NME-RVPN в составе маршрутизатора Cisco Integrated Services Router 2800/3800 обеспечивает эффективную реализацию множества сценариев сертифицированной защиты, включая:

- межсетевые взаимодействия;
- защищенный доступ удаленных и мобильных пользователей;
- защиту беспроводных сетей;
- защиту мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь);
- защиту платежных систем и систем управления технологическими процессами в производстве и на транспорте.

Сценарии защиты межсетевых взаимодействий (Site-to-Site VPN) применяются для защиты коммуникаций территориально распределенных корпоративных сетей через публичные (открытые, не заслуживающие доверия) сети/каналы связи (рис.10.10).

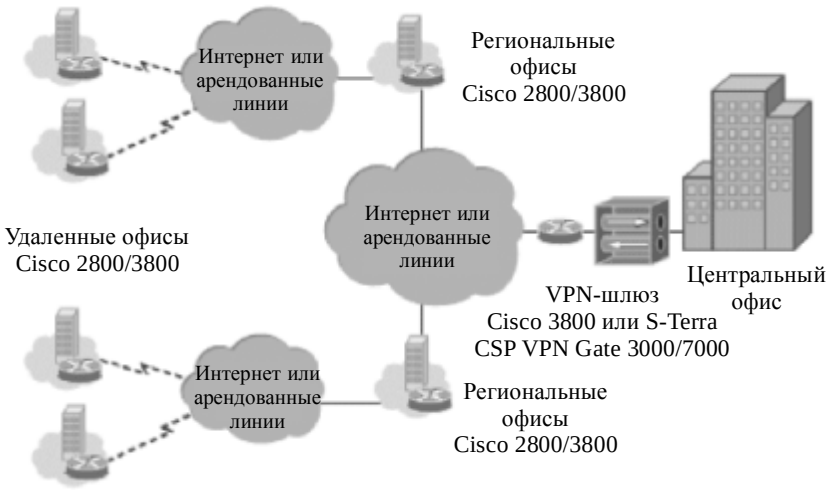

Рис.10.10. Использование VPN-туннелей для создания защищенной корпоративной сети

По сути, применение VPN-решений для этих целей не должно приводить к понижению требований к характеристикам непосредственно канала передачи данных, таких, как поддержка множественности протоколов, высокая надежность, большая масштабируемость. Наоборот, современные VPN-решения должны обеспечивать высокую ценовую эффективность и большую гибкость в реализации таких требований.

Высокую ценовую эффективность можно получить, например, за счет возможности использовать публичные каналы для передачи информации, что ранее было недоступно. Использование для этой цели маршрутизаторов Cisco Integrated Services Router в полной мере выполняет поставленную выше задачу.

Вопросы для самоконтроля

1. Что такое виртуальные защищенные сети VPN (Virtual Private Network)?
2. Сформулируйте концепцию построения виртуальных защищенных сетей VPN.
3. Объясните понятия «виртуальный защищенный туннель», «туннелирование» и «инкапсуляция».
4. Дайте развернутые определения таких устройств VPN, как VPN-клиент, VPN-сервер и VPN-шлюз безопасности.
5. Поясните особенности структуры и функционирования двух основных схем виртуальных защищенных каналов.
6. Каковы функции инициатора туннеля и терминатора туннеля?
7. Какие методы используют для обеспечения безопасности сетей VPN?
8. Опишите классификацию сетей VPN по рабочему уровню модели взаимодействия открытых систем OSI (Open Systems Interconnection).
9. Каковы основные варианты архитектуры сетей VPN? Дайте пояснение для каждого из трех основных вариантов.
10. Укажите основные виды технической реализации VPN и дайте пояснения для каждого из них.
11. Какие российские компании выпускают VPN-продукты в настоящее время?
12. Опишите возможности и основные характеристики семейства VPN-продуктов CSP VPN 3.0 российской компании «С-Терра СиЭсПи».

Часть 4. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Для успешного использования современных информационных технологий необходимо надежное и эффективное управление средствами обеспечения информационной безопасности. И если раньше задача заключалась в управлении средствами защиты рабочих станций, серверов, маршрутизаторов и сетей, то сейчас требуется обеспечить комплексное управление безопасностью корпоративных информационных систем.

Важным аспектом управления информационной безопасностью является строгое соблюдение технических и организационно-правовых требований, предъявляемых к средствам и системам защиты информации. Эти требования сформулированы в ряде отечественных и международных стандартов по информационной безопасности, а также в Руководящих документах (РД) по технической защите информации Государственной технической комиссии (ГТК) России.

Глава 11. Управление средствами обеспечения информационной безопасности

Нужно не только овладеть мудростью,
но и уметь пользоваться ею.
Цицерон

Корпоративная информационная система - это активный инструмент ведения бизнеса. Эффективная деятельность современного предприятия невозможна без единой корпоративной информационной системы, объединяющей различные бизнес-процессы предприятия. Динамичное развитие бизнеса обусловливает быстрый рост и усложнение корпоративных информационных систем, расширяются их функции и набор предоставляемых сервисов.

Ввиду растущей сложности современного бизнеса компаниям приходится постоянно внедрять все новые и новые технологии, устанавливая более мощное и качественное оборудование. При этом необходимо обеспечить безопасность корпоративных бизнес-процессов, а также надежное и эффективное управление средствами информационной безопасности.

11.1. Задачи управления информационной безопасностью

Важнейшим компонентом корпоративной системы является система управления средствами информационной безопасности предприятия. Сформулируем основные задачи системы управления средствами информационной безопасности предприятия.

Функционально такая система должна решать следующие основные задачи:

- централизованное управление всеми программными и техническими средствами защиты информации;
- управление политикой безопасности в рамках КИС предприятия, формирование локальных политик безопасности (ЛПБ) отдельных устройств и доведения ЛПБ до всех устройств защиты информации;
- распространение обновлений программного обеспечения, а также дополнительных программных средств на рабочие станции и серверы;
- управление конфигурациями объектов и субъектов доступа;
- управление правами доступа к активным сетевым устройствам, рабочим станциям и серверам;
- предоставление сервисов защиты распределенным прикладным системам, регистрация защищенных приложений и их ресурсов;
- управление криптосредствами, в частности управление криптоключами (ключевая инфраструктура);
- событийное протоколирование, включающее настройку выдачи логов на разные устройства, управление уровнем детализации логов, управление составом событий, по которым ведется протоколирование;
- аудит безопасности информационной системы, который обеспечивает получение и оценку объективных данных о текущем состоянии защищенности информационной системы; иногда под аудитом безопасности понимают анализ логов, поиск нарушителей и дыр в существующей системе, однако эти функции покрываются, скорее, задачами управления логами;
- мониторинг безопасности системы, обеспечивающий получение информации в реальном времени о состоянии, активности устройств и о событиях с контекстом безопасности, происходящих в устройствах, например о потенциальных атаках.

При построении системы управления средствами информационной безопасности предприятия возникает проблема организации взаимодействия и комплексирования традиционных систем управления КИС и систем управления информационной безопасностью. Для решения этой проблемы применяются два основных подхода.

Первый подход заключается в интеграции средств сетевого и системного управления с механизмами управления средствами защиты. Средства сетевого и системного управления ориентированы в первую очередь на управление сетью и информационными системами, т.е. поддерживают традиционные действия и услуги: управление учетными записями пользователей, управление ресурсами и событиями, маршрутизацию, производительность и т.п. Ряд компаний Cisco Systems, IBM Tivoli Systems, Computer Associates, Hewlett Packard пошли по пути интеграции механизмов управления средств защиты в традиционные системы управления. Однако такие комплексные системы управления часто отличаются высокой стоимостью и, кроме того, некоторые аспекты управления безопасностью остаются за пределами внимания этих систем.

Второй подход заключается в использовании средств, предназначенных для решения только задачи управления безопасностью. Например, Open Security Manager (OSM) от Check Point Software Technologies дает возможность централизованно управлять корпоративной политикой безопасности и инсталлировать ее на сетевые устройства по всей компании. Продукт OSM является одной из основных компонент технологии OPSEC (Open Platform for Secure Enterprise Connectivity), разработанной компанией CheckPoint, он создает интерфейс для управления устройствами сетевой безопасности различных производителей (например, Cisco, Bay, 3Com).

Для обеспечения безопасности информационных ресурсов предприятия средства защиты информации обычно размещаются непосредственно в корпоративной сети. Межсетевые экраны контролируют доступ к корпоративным ресурсам, отражая атаки злоумышленников извне, а шлюзы виртуальных частных сетей (VPN) обеспечивают конфиденциальную передачу информации через открытые глобальные сети, в частности Интернет. Для создания надежной эшелонированной защиты в настоящее время применяются также такие средства безопасности, как системы обнаружения и предотвращения вторжений IPS (Intrusion Prevention Systems), средства контроля контента, антивирусные системы и др.

К сожалению, практически невозможно найти компанию-производителя, которая могла бы предоставить потребителю за приемлемую цену полный набор средств (от аппаратных до программных) для построения современной корпоративной информационной системы. Поэтому большинство КИС компаний обычно построены на основе программных и аппаратных средств, поставляемых различными производителями. Каждое из этих средств требует тщательного и специфического конфигурирования, отражающего взаимосвязи между пользователями и доступными им ресурсами.

Чтобы обеспечить в гетерогенной КИС надежную защиту информации, нужна рационально организованная система управления безопасностью КИС, которая обеспечила бы безопасность и правильную настройку каждого компонента КИС, постоянно отслеживала происходящие изменения, устанавливала «заплатки» на найденные в системе бреши, контролировала работу пользователей. Очевидно, что чем разнороднее информационная система, тем сложнее обеспечить управление ее безопасностью.

Опыт ведущих предприятий-производителей средств информационной безопасности показывает, что компания сможет успешно реализовать свою политику безопасности в распределенной корпоративной информационной системе, если управление безопасностью будет централизованным и не будет зависеть от используемых ОС и прикладных систем. Кроме того, система регистрации событий, происходящих в КИС (события НСД, изменение привилегий пользователей и т.д.), должна быть единой и позволять администратору составить полную картину происходящих в КИС изменений.

Для решения ряда задач управления безопасностью требуется применение единых вертикальных инфраструктур типа каталога X.500. Например, политика сетевого доступа требует знания идентификаторов пользователей. Эта информация нужна и другим приложениям, например в системе кадрового учета, в системе однократного доступа к приложениям (single sign-on) и т.д. Дублирование одних и тех же данных приводит к необходимости синхронизации, увеличению трудоемкости и возможной путанице. Поэтому, чтобы избежать такого дублирования, часто используют единые вертикальные инфраструктуры. К таким вертикальным структурам, используемым различными пользовательскими подсистемами, работающими на разных уровнях OSI/ISO, относятся:

- инфраструктуры управления открытыми ключами PKI;
- каталоги (например, идентификаторов пользователей и других сведений о пользователях, необходимых в системах управления доступом); каталоги часто используются не только как хранилища данных, в них также часто располагаются политики доступа, сертификаты, списки доступа и др.);
- системы аутентификации (обычно RADIUS, серверы TACACS, TACACS+);
- системы событийного протоколирования, мониторинга и аудита (следует отметить, что эти системы не всегда вертикальны, часто специализируются и работают автономно в интересах конкретных подсистем).

Учитывая, что методология централизованного управления достаточно полно отражает современные тенденции развития технологий обеспечения информационной безопасности КИС, российская компания «НПО Информзащита» разработала систему комплексного управления безопасностью (КУБ). В системе КУБ реализуется оригинальная технология управления безопасностью. Особенность этой технологии заключается в том, что она предлагает полноценный организационный подход к решению проблемы управления безопасностью,

поддержанный программными средствами. Использование этой технологии позволяет управлять безопасностью корпоративной информационной системы и обеспечить защиту нематериальных активов компании [22].

Основываясь на методологии централизованного управления, российская компания TrustWorks Systems разработала эффективную систему глобального управления безопасностью GSM (Global Security Management) для корпоративной информационной системы. Эта отечественная система управления информационной безопасностью КИС нашла широкое практическое применение и описывается в разделах 11.2, 11.3 и 11.5.

Рассмотрим решения следующих задач управления безопасностью: управление обновлениями программных средств; управление конфигурациями объектов и субъектов доступа; управление учетными записями и правами доступа к активным сетевым устройствам, рабочим станциям и серверам.

Управление обновлениями программных средств. Регулярное обновление программных средств корпоративной информационной системы позволяет избежать угрозы эксплуатации злоумышленниками известных уязвимостей программного обеспечения. При этом увеличение сложности программного обеспечения и количества компонентов приводит к тому, что практически ежедневно выходят несколько критичных обновлений, которые должны быть обязательно установлены на все рабочие станции и серверы предприятия.

Кроме того, каждое обновление должно быть предварительно проверено на совместимость с остальными программными средствами, используемыми на предприятии (например, предварительной установкой на тестовые рабочие станции).

Подсистемы управления обновлениями позволяют автоматизировать следующие задачи:

- автоматическое получение обновлений с сайтов производителей ПО;
- организация централизованного хранилища обновлений;
- возможность назначения обновлений определенным рабочим станциям и серверам или группам рабочих станций и серверов;
- автоматическая установка выбранных обновлений на рабочие станции пользователей.

Управление конфигурациями. Централизованное управление конфигурацией рабочих станций, серверов, активного сетевого оборудования позволяет существенно сократить затраты на обеспечение актуальной конфигурации оборудования информационной системы предприятия.

Использование централизованного управления рабочими станциями и серверами позволяет:

- автоматически распространять приложения на рабочие станции и серверы;
- создавать типовые образы рабочих станций и серверов для быстрого ввода в эксплуатацию новых единиц техники;
- поддерживать соответствие локальных настроек политике безопасности организации.

Централизованное управление сетевым оборудованием позволяет:

- централизованно хранить конфигурации активного сетевого оборудования;
- распределять административные роли по типам и группам устройств;
- задавать высокоуровневые изменения сетевой инфраструктуры, которые будут автоматически преобразованы в изменения конфигураций конкретных сетевых устройств;
- осуществлять мониторинг сетевых устройств;
- производить откат неудачных изменений конфигурации.

Системы централизованного управления непосредственно зависят от систем централизованного управления учетными записями и правами доступа, а также систем администрирования доступа к сетевому оборудованию.

Разграничение доступа к сетевому оборудованию. Подсистема разграничения доступа к сетевому оборудованию включает в себя:

- централизованное управление доступом к сетевому оборудованию;
- разграничение доступа к командам сетевого оборудования.

Злонамеренные действия или ошибки администратора сетевого оборудования могут привести к нарушению конфиденциальности данных, передаваемых по корпоративной сети или к другим инцидентам информационной безопасности.

В больших информационных системах очень сложно осуществлять контроль и управление административным доступом для каждого отдельного сетевого устройства. Это не позволяет в полной мере реализовать требования политики безопасности и предполагает большие трудозатраты со стороны системных администраторов, обусловленные необходимостью управления разрозненными локальными базами учетных записей.

Системы разграничения доступа к сетевому оборудованию, построенные на основе средств аутентификации, авторизации и учета - AAA-серверов и средств делегирования административных полномочий, позволяют решить задачи по разграничению доступа к конкретным командам управления, ведению журналов, а также по созданию централизованной базы учетных записей администраторов сетевого оборудования.

При организации доступа к сетевому оборудованию модель AAA подразумевает выполнение соответствующих процедур:

- аутентификация (Authentication) - процедура проверки данных учетной записи с целью установки соответствия пользователя множеству зарегистрированных субъектов доступа;
- авторизация (Authorization) - процедура установки полномочий пользователя и выделения ресурсов;

• учет (Accounting) - процедура учета действий, выполняемых пользователем на протяжении сеанса доступа.

AAA-серверы могут представлять собой как программные средства, так и программно-аппаратные комплексы.

В настоящее время наибольшую популярность получили следующие технологии, реализующие модель AAA: Remote Authentication in Dial-In User Service (RADIUS) и Terminal Access Controller Access-Control System (TACACS+).

Средства делегирования административных полномочий представляют собой отдельный класс средств разграничения административного доступа к сетевому оборудованию. Делегирование административных полномочий обеспечивается путем контроля административного доступа и ролевого разграничения доступа к конфигурационным командам.

Задача ролевого разграничения доступа к конфигурационным командам реализуется инструментальными комплексами в три этапа:

• сканирование активного сетевого оборудования на предмет выявления всех конфигурационных команд;

• анализ полученных результатов и создание политики безопасности с целью разграничения доступа к конфигурационным командам на основе ролей;

• создание конфигурации для ролевого разграничения доступа к командам.

Подсистема разграничения доступа к сетевому оборудованию может осуществлять взаимодействие с рядом других подсистем. В частности, взаимодействие с корпоративным LDAP-каталогом позволяет создать единое, в рамках организации, пространство учетных записей и упростить управление ими (рис.11.1).

Рис.11.1. Использование корпоративного LDAP-каталога для управления учетными записями

Взаимодействие с системами мониторинга позволяет вести централизованный контроль за действиями администраторов на основе данных учета и предпринимать своевременные меры по предотвращению инцидентов информационной безопасности.

Задачи управления криптосредствами, аудита и мониторинга безопасности КИС, событийного протоколирования и ряд других решаются системой управления информационной безопасности с привлечением соответствующих подсистем комплексной системы защиты информации (см. раздел 3.3).

11.2. Архитектура управления информационной безопасностью КИС

Компания TrustWorks Systems разработала систему централизованного управления безопасностью КИС с применением глобальной и локальных политик безопасности. В основе централизованного управления безопасностью КИС лежит концепция глобального управления безопасностью GSM (Global Security Management).

11.2.1. Концепция глобального управления безопасностью GSM

Концепция GSM позволяет построить комплексную систему управления и защиты информационных ресурсов предприятия со следующими свойствами:

• управление всеми существующими средствами защиты на базе политики безопасности предприятия, обеспечивающее целостность, непротиворечивость и полноту набора правил защиты для всех ресурсов предприятия (объектов политики безопасности) и согласованное исполнение политики безопасности средствами защиты, поставляемыми разными производителями;

• определение всех информационных ресурсов предприятия через единый (распределенный) каталог среды предприятия, который может актуализироваться как за счет собственных средств описания ресурсов, так и посредством связи с другими каталогами предприятия (в том числе по протоколу LDAP);

• централизованное, основанное на политике безопасности (policy-based) управление локальными средствами защиты информации;

• строгая аутентификация объектов политики в среде предприятия с использованием PKCS#11-токенов и инфраструктуры открытых ключей PKI, включая возможность применения дополнительных локальных средств аутентификации LAS (по выбору потребителя);

• расширенные возможности администрирования доступа к определенным в каталоге ресурсам предприятия или частям всего каталога (с поддержкой понятий групп пользователей, доменов, департаментов предприятия), управление ролями как набором прав доступа к ресурсам предприятия, введение в политику безопасности элементов косвенного определения прав через атрибуты прав доступа (credentials);

• обеспечение подотчетности (регистрация всех операций взаимодействий распределенных объектов системы в масштабах корпоративной сети) и аудита, мониторинга безопасности, тревожной сигнализации;

• интеграция с системами общего управления, инфраструктурными системами безопасности (PKI, LAS, IPS).

В рамках данной концепции термин «управление, основанное на политике безопасности PBM (Policy based management)» определяется как реализация набора правил управления, сформулированных для бизнес-объектов предприятия, которая гарантирует полноту охвата бизнес области объектами и непротиворечивость используемых правил управления.

Система управления GSM, ориентированная на управление безопасностью предприятия на принципах PBM, удовлетворяет следующим требованиям:

• политика безопасности предприятия представляет собой логически и семантически связанную, формируемую, редактируемую и анализируемую как единое целое структуру данных;

• политика безопасности предприятия определяется в едином контексте для всех уровней защиты как единое целое сетевой политики безопасности и политики безопасности информационных ресурсов предприятия;

• для облегчения администрирования ресурсов и политики безопасности предприятия число параметров политики минимизируется.

Для того чтобы минимизировать число параметров политики, используются следующие приемы:

1. Групповые определения объектов безопасности.
2. Косвенные определения, например определения на основе верительных (credential) атрибутов.
3. Мандатное управление доступом (в дополнение к фиксированному доступу), когда решение о доступе определяется на основе сопоставления уровня доступа, которым обладает субъект, и уровня конфиденциальности (критичности) ресурса, к которому осуществляется доступ.

Система управления GSM обеспечивает разнообразные механизмы анализа политики безопасности за счет средств многокритериальной проверки соответствия политики безопасности формальным моделям концепции безопасности предприятия.

11.2.2. Глобальная и локальная политика безопасности

Согласно концепции GSM организация централизованного управления безопасностью КИС основана на следующих принципах:

• управление безопасностью корпоративной информационной системы должно осуществляться на уровне глобальной политики безопасности (ГПБ);

• ГПБ должна соответствовать бизнес-процессам компании. Для этого свойства безопасности объектов и требуемые сервисы безопасности должны быть описаны с учетом их бизнес-ролей в структуре компании;

• для отдельных средств защиты формируются локальные политики безопасности. Трансляция ЛПБ должна осуществляться автоматически на основе анализа правил ГПБ и топологии защищаемой сети.

Глобальная политика безопасности корпоративной системы представляет собой конечное множество правил безопасности (security rules) (рис.11.2),

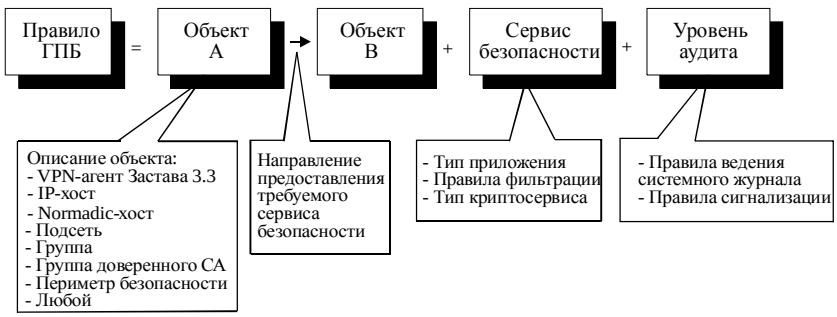

Рис.11.2. Структура правила глобальной политики безопасности

которые описывают параметры взаимодействия объектов корпоративной сети в контексте информационной безопасности:

- необходимый для соединения сервис безопасности: правила обработки, защиты и фильтрации трафика;
- направление предоставления сервиса безопасности;
- правила аутентификации объектов;
- правила обмена ключами;
- правила записи результатов событий безопасности в системный журнал;
- правила сигнализации о тревожных событиях и др.

При этом объектами ГПБ могут быть как отдельные рабочие станции и подсети, так и группы объектов, которые могут включать в себя целые структурные подразделения компании (например, отдел маркетинга или финансовый департамент) или даже отдельные компании (входящие, например, в холдинг). Политика безопасности для каждого объекта в группе автоматически реплицируется всем объектам группы.

Задачи защиты бизнес-объектов распределенной корпоративной системы можно сформулировать в терминах правил, поскольку сетевое взаимодействие можно представить как простую передачу информации между субъектом Subj и объектом Obj доступа на основе некоторого сетевого сервиса защиты SecSrv, настроенного при помощи параметров P. В результате глобальная политика безопасности предприятия представляется как набор правил вида (Subj, Obj, SecSrv (P)). При этом отсутствие правила для объекта Obj означает запрет любого доступа к данному Obj.

Для простоты определения целей безопасности предприятия в GSM предусмотрено два типа объектов, выступающих в качестве Subj и Obj. Это пользователь (U) и ресурс (R). Ресурс R может быть информационным (IR) или сетевым (NR).

Пользователь и ресурс могут выступать в любой из форм агрегации, поддерживаемых в системе: группы, домены, роли, департаменты, разделы каталога.

Пример. Правило (U, IR, S1) представляет собой правило защиты S1, обеспечиваемое при доступе пользователя U к информационному ресурсу IR. Правило (IR1, IR2, S2) означает разрешение сетевого взаимодействия двух информационных модулей (программ) с необходимостью обеспечения свойств защиты S2.

Политика по умолчанию для доступа к любому защищаемому объекту корпоративной системы представляет собой запретительное правило**:** *все, что не разрешено явно*, - *запрещено*. Такое правило обеспечивает полноту защиты информации в сети предприятия и априорное отсутствие «дыр» в безопасности.

Чтобы обеспечить взаимодействие устройств в сети, для всех устройств сети создается и доставляется (в общем случае не по каналам сети) *стартовая конфигурация*, содержащая необходимые правила настройки устройств только для их централизованного управления, -стартовая политика безопасности устройства.

Правила ГПБ могут быть распространены как на сетевые взаимодействия, так и на функции контроля и управления самой системы.

Функционально правила ГПБ разбиты по группам:

- *правила VPN* - реализуются при помощи протоколов IPSec; агентом исполнения данного правила является драйвер VPN в стеке клиентского устройства или шлюза безопасности (IP1, IP2, VPNRule);
- *правила пакетной фильтрации, включая NAT,* - обеспечивают пакетную фильтрацию типа stateful и stateless; исполнение этих правил обеспечивают те же агенты, что исполняют VPN-правила (IP1, IP2, PacketRule);
- *proxy-правила, включая антивирусную защиту налету*, - отвечают за фильтрацию трафика, передаваемого под управлением заданных прикладных протоколов; исполнительным агентом этих правил является proxy-агент, например (User, Protocol, ProxyRule) или (Application, Protocol, ProxyRule);
- *правила аутентифицированного/авторизованного доступа, включая правила Single Sign-On,* - управление доступом Single Sign-On обеспечивает данному пользователю работу на едином пароле или другой аутентификационной информации со многими информационными ресурсами; отсюда легко видеть, что символическая запись правила сетевого доступа легко распространяется на single sign-on (User, Application, Authentication Scheme). Правила этой группы могут комбинированно исполняться агентами различного уровня - от VPN драйвера до proxy-агентов; кроме того, агентами исполнения таких правил могут быть системы аутентификации запрос-отклик и продукты третьих разработчиков;
- *правила, отвечающие за сигнализацию и событийное протоколирование,* - политика протоколирования может оперативно и централизованно управляться агентом протоколирования; исполнителями правил являются все компоненты системы.

Различие между правилами, реализующими глобальную политику безопасности в сети, и правилами, реализующими локальную политику безопасности конкретного устройства, заключается в том, что в правилах группы ГПБ объекты и субъекты доступа могут быть распределены произвольным образом в пределах сети, а правила группы ЛПБ, включая субъекты и объекты ЛПБ, предназначены и доступны только в пределах пространства одного из сетевых устройств.

Набор правил ГПБ является логически целостным и семантически полным описанием политики безопасности в масштабах КИС, на основе которой может строиться локальная политика безопасности отдельных устройств.

Любому средству защиты, реализующему какой-либо сервис информационной безопасности, необходима для выполнения его работы *локальная политика безопасности*, т.е. точное описание настроек

для корректной реализации правил аутентификации пользователей, управления доступом, защиты трафика и др.

При традиционном подходе администратору приходится отдельно настраивать каждое средство защиты или реплицировать какие-то простейшие настройки на большое число узлов с последующей их корректировкой. Очевидно, что это неизбежно приводит к большому числу ошибок администрирования и, как следствие, существенному снижению уровня защищенности корпоративной сети.

После формирования администратором глобальной политики безопасности Центр управления на основе интерпретации ГПБ автоматически вычисляет и, если это необходимо, корректирует отдельные ЛПБ для каждого средства защиты и автоматически загружает необходимые настройки в управляющие модули соответствующих средств защиты.

В целом локальная политика безопасности сетевого устройства включает в себя полный набор *правил* разрешенных соединений данного устройства, исполняемых для обеспечения какой-либо информационной услуги с требуемыми свойствами защиты информации.

11.3. Функционирование системы управления информационной безопасностью КИС

Структурно-продуктная линия системы управления GSM подразделяется на агентов безопасности (Trusted Agent), центр управления (Trusted GSM Server) и консоль управления (Trusted GSM Console). Общая структурная схема решения показана на рис.11.3.

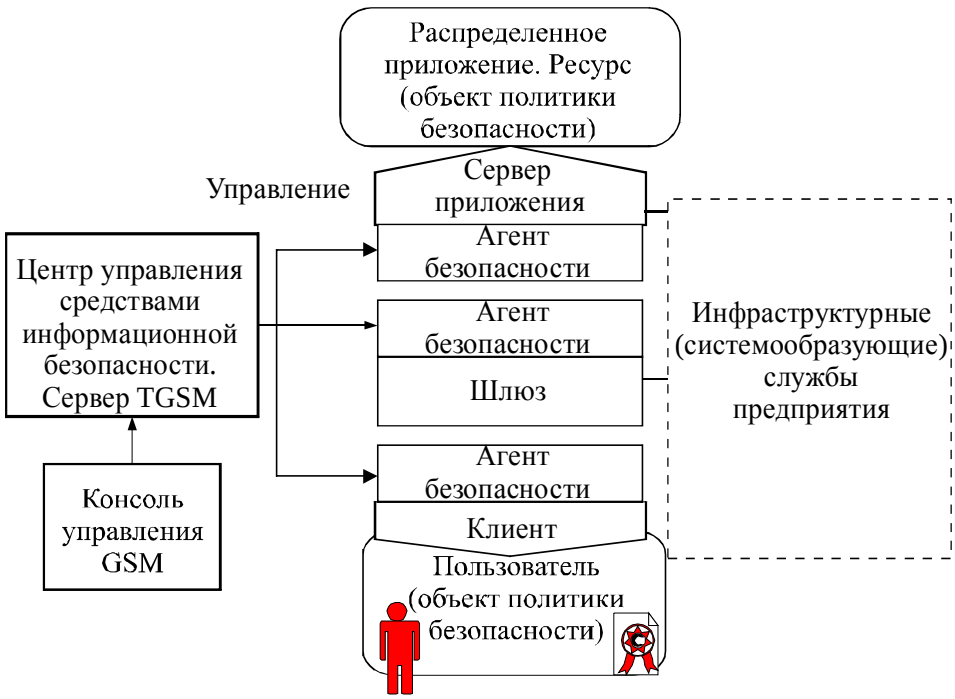

Рис.11.3. Общая структурная схема системы управления средствами информационной безопасности

11.3.1. Назначение основных средств защиты

Агент безопасности (Trusted Agent), установленный на *персональном компьютере клиента*, ориентирован на защиту индивидуального пользователя, выступающего, как правило, клиентом в приложениях клиент-сервер.

Агент безопасности, установленный на *сервере приложений*, ориентирован на обеспечение защиты серверных компонент распределенных приложений.

Агент безопасности, установленный на *шлюзовом компьютере*, обеспечивает развязку сегментов сети внутри предприятия или между предприятиями.

Центр управления (Trusted GSM Server) обеспечивает описание и хранение глобальной политики безопасности в масштабах сети, трансляцию глобальной политики в локальные политики безопасности устройств защиты, загрузку устройств защиты и контроль состояний всех агентов системы. Для организации распределенной схемы управления безопасности предприятия в системе GSM предусматривается установка нескольких (до 65535) серверов GSM.

Консоль управления (Trusted GSM Console) предназначена для организации рабочего места администратора (администраторов) системы. Для каждого из серверов GSM может быть установлено несколько консолей, каждая из которых настраивается согласно ролевым правам каждого из администраторов системы GSM.

Локальный агент безопасности (Trusted Agent) представляет собой программу, размещаемую на оконечном устройстве (клиенте, сервере, шлюзе) и выполняющую следующие функции защиты:

- аутентификацию объектов политики безопасности, включая интеграцию различных сервисов аутентификации;
- определение пользователя в системе и событий, связанных с данным пользователем;
- обеспечение централизованного управления средствами безопасности и контроля доступа;
- управление ресурсами в интересах приложений, поддержку управления доступом к ресурсам прикладного уровня;
- защиту и аутентификацию трафика;
- фильтрацию трафика;
- событийное протоколирование, мониторинг, функцию тревожной сигнализации.

Дополнительные функции Trusted Agent (разрабатываются в составе решения GSM):

- поставка криптосервиса (multiple concurrent pluggable modules);
- управление периметрами single sign-on (как подзадача аутентификации пользователей);
- сервис в интересах защищенных приложений (криптосервис, сервис доступа к PKI, доступ к управлению безопасностью);
- сжатие трафика (IPcomp, pluggable module);
- управление резервированием сетевых ресурсов (QoS);
- функции локального агента сетевой антивирусной защиты.

Центральным элементом локального агента является процессор локальной политики безопасности (LSP processor), интерпретирующий локальную политику безопасности и распределяющий вызовы между остальными компонентами.

11.3.2. Защита ресурсов

Аутентификация и авторизация доступа. В рамках решения реализуется ряд различных по функциональности схем аутентификации, каждая из которых включает тип аутентификации и способ (механизм) идентификации объектов.

Для выбора типа аутентификации предусмотрены следующие возможности: аутентификация пользователя при доступе к среде GSM или локальной операционной системе, аутентификация пользователя при доступе в сеть (сегмент сети), взаимная сетевая аутентификация объектов (приложение-приложение). Для выбора способа идентификации предусмотрены следующие варианты, предполагающие их любое совместное использование: токен (смарт-карта), пароль, «внешняя» аутентификация.

Контроль доступа при сетевых взаимодействиях. При инициализации защищенного сетевого соединения от локальной операционной системы или при получении запроса на установление внешнего соединения локальные агенты безопасности Trusted Agent на концах соединения (и/или на промежуточном шлюзе) обращаются к ЛПБ устройства и проверяют, разрешено ли установление данного соединения. В случае если такое соединение разрешено, обеспечивается требуемый сервис защиты данного соединения, если запрещено - сетевое соединение не предоставляется.

Контроль доступа на уровне прикладных объектов. Для незащищенных распределенных приложений в GSM обеспечивается сервис разграничения прав доступа на уровне внутренних объектов данного приложения. Контроль доступа на уровне объектов прикладного уровня обеспечивается за счет применения механизма proxy. Proxy разрабатывается для каждого прикладного протокола. Протокол http является предустановленным.

Для построения распределенной схемы управления и снижения загрузки сети в GSM используется архитектура распределенных прокси-агентов «lightweight proxy» (Proxy Module в составе Trusted Agent), каждый из которых:

- имеет абстрактный универсальный интерфейс, обеспечивающий модульное подключение различных proxy-фильтров;
- имеет интерфейс к системе управления, но использует временный кэш для управления параметрами фильтрации, которая управляется обобщенными правилами типа:

- аутентифицировать субъект *X* в приложении-объекте *Y*;
- разрешить доступ субъекту *X* к объекту *Y* с параметрами *P*;
- запретить доступ субъекту *X* к объекту *Z*.

Семантика правил управления proxy-фильтром и описания субъектов и объектов доступа зависят от конкретного прикладного протокола, однако центр управления имеет возможность регистрировать proxy-фильтры и обеспечивать управления ими в контексте общей глобальной политики безопасности.

ProxyAgent может быть установлен на шлюзе безопасности, непосредственно на сервере, исполняющем контролируемые приложения, и на клиентском месте системы.

11.3.3. Управление средствами защиты

Важнейшим элементом решения TrustWorks является централизованная, основанная на политике (policy based) система управления средствами сетевой и информационной безопасности масштаба предприятия. Эта система обеспечивает следующие качественные потребительские характеристики:

- высокий уровень защищенности системы управления (путем выделения защищенного периметра управления внутри сети предприятия);
- расширяемость системы управления информационной безопасностью;
- высокий уровень надежности системы управления и ключевых ее компонент;
- интеграцию с корпоративными системами общего сетевого и информационного управления;
- простую, интуитивно воспринимаемую, эргономичную и инфраструктурную среду описания, формирования, мониторинга и диагностики политики безопасности масштаба предприятия (enterprise level policy based management).

Управление осуществляется специальным программным обеспечением администратора - консолью управления (Trusted GSM Console). Количество и функции каждого из экземпляров установленного в системе ПО Trusted GSM Console задаются главным администратором системы в зависимости от организационной структуры предприятия. Для назначения функций каждого из рабочих мест Trusted GSM Console используется ролевой механизм разграничения прав по доступу к функциям управления (менеджмента) системы.

В зависимости от вида управляемых объектов набор управляющих функций в GSM можно условно разбить на 3 категории:

- управление информационным каталогом;
- управление пользователями и правами доступа;
- управление правилами ГПБ (GSP - Global Security Policy).

Функции управления информационным каталогом определяют информационную составляющую GSM:

- формирование разделов каталога;
- описание услуг каталога;
- назначение и контроль сетевых ресурсов, требуемых для выполнения услуги;
- регистрация описания услуги;
- контроль состояния услуг или разделов каталога услуг;
- мониторинг исполнения услуг;
- подготовка и пересылка отчетов (протоколов) по состоянию каталога.

Для управления правами доступа пользователей системы к услугам (информационным или сетевым ресурсам) GSM обеспечивает следующие функции:

- формирование групп пользователей по ролям и/или привилегиям доступа к услугам системы;
- формирование иерархических агрегаций пользователей по административным, территориальным или иным критериям (домены и/или департаменты);
- формирование ролей доступа пользователей к услугам (информационным или сетевым ресурсам);
- назначение уровней секретности для услуг и пользователей системы (поддержка мандатного механизма разграничения прав);
- назначение фиксированных прав доступа группам, ролям, агрегациям пользователей или отдельным пользователям системы к информационным или сетевым ресурсам системы;
- подготовка и пересылка отчетов (протоколов) по доступу пользователей к услугам системы;
- подготовка и пересылка отчетов (протоколов) по работе администраторов системы.

Правила ГПБ ставят в соответствие конкретные свойства защиты (как для сетевых соединений, так и для доступа пользователей к информационным услугам) предустановленным уровням безопасности системы. Контроль за соблюдением правил ГПБ выполняет специальный модуль в составе сервера системы - *Security Policy Processor*, обеспечивающий следующие функции системы:

- определение каждого из уровней безопасности набором параметров защиты соединений, схемы аутентификации и разграничения прав;
- назначение уровней безопасности конкретным услугам или разделам каталога услуг;
- назначение уровней безопасности пользователям или любым агрегациям пользователей системы (группам, ролям, доменам, департаментам);
- контроль за целостностью ГПБ (полнотой правил);
- вычисление политик безопасности ЛПБ локальных устройств защиты - агентов безопасности - и контроль их исполнения;
- контроль за исполнением ГПБ по различным критериям;
- подготовка и пересылка отчетов (протоколов) по состоянию системы и всех попыток нарушения ГПБ.

Каждый из администраторов системы аутентифицируется и работает с системой через Trusted GSM Console согласно предустановленным для него правам (на каталог ресурсов или его часть, на определенный ролями набор функций управления, на группы или другие наборы пользователей). Все действия любого из администратора протоколируются и могут быть попарно контролируемы.

11.4. Обзор современных систем управления безопасностью

Задачи управления безопасностью корпоративных информационных систем стали актуальными в эпоху массового распространения клиент-серверных технологий и децентрализованных вычислений. Принимая этот вызов времени, поставщики стали разрабатывать продукты, позволяющие решать задачи управления безопасностью распределенных информационных систем. Лидерами на рынке средств управления безопасностью распределенных информационных систем являются такие компании, как Cisco Systems, IBM Tivoli, Check Point и др. Ниже рассматриваются некоторые конкретные реализации средств управления безопасностью.

11.4.1. Централизованное управление безопасностью, реализованное в продуктах Застава

Принцип централизованного управления безопасностью корпоративной системы, разработанный компанией Trust Works Systems (см. раздел 11.2) и реализованный в продуктах Застава компании «ЭЛВИС+», основывается на следующих концептуальных положениях:

- управление безопасностью корпоративной системы должно осуществляться на уровне глобальной политики безопасности - наборе правил безопасности для сколь угодно сложного множества взаимодействий между разнообразными объектами корпоративной системы, а также между объектами корпоративной системы и внешними объектами;
- ГПБ должна максимальным образом соответствовать бизнес-процессам компании; для этого должен существовать способ описания свойств безопасности объектов и требуемых для их реализации сервисов безопасности, основанный на их бизнес-ролях в структуре компании;
- формирование локальных политик безопасности для отдельных средств защиты и их трансляция должны осуществляться автоматически на основе анализа правил ГПБ и топологии защищаемой сети с обязательной автоматической проверкой их корректности, целостности и непротиворечивости ГПБ (рис.11.4).

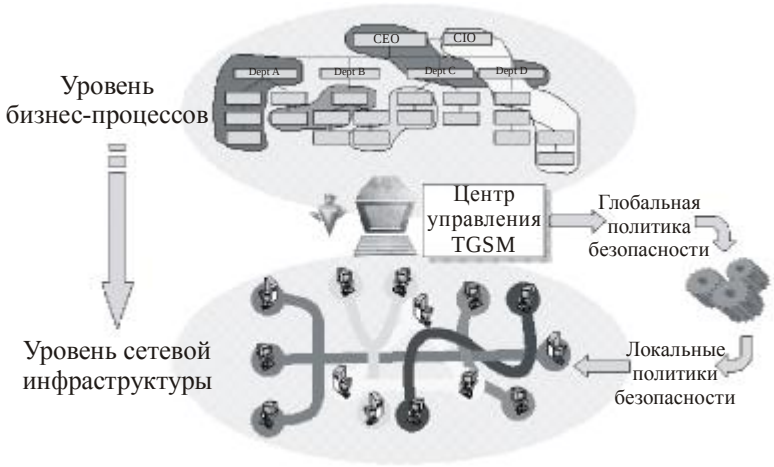

Рис.11.4. Структура централизованного управления безопасностью КИС

Объектами глобальной политики безопасности могут быть как отдельные рабочие станции и подсети, так и группы объектов, которые могут включать в себя целые структурные подразделения компании (например, отдел маркетинга или финансовый департамент) или даже отдельные компании (входящие, например, в холдинг). Администратору безопасности не нужно заботиться о формировании политики безопасности для каждого объекта в группе - заданная политика автоматически реплицируется всем объектам группы.

Локальная политика безопасности необходима для нормального функционирования любого средства защиты, реализующего какой-либо сервис информационной безопасности. Локальная политика безопасности представляет собой точное описание настроек средства защиты для корректной реализации правил аутентификации пользователей, управления доступом, защиты трафика и др.

Решение на базе VPN Застава реализует эффективный подход к проблеме обеспечения безопасности корпоративной системы: после формирования ГПБ администратором центр управления TGSM на основе ее интерпретации автоматически вычисляет и, если это необходимо, корректирует отдельные ЛПБ для каждого средства защиты и автоматически загружает необходимые настройки в управляющие модули соответствующих средств защиты:

- в автоматическом режиме по протоколу PMP (Policy Management Protocol), являющемуся стандартным расширением протокола IKE в виде сообщения в формате PKCS#7;
- в ручном режиме путем выдачи ЛПБ на PKCS#11-совместимый идентификатор пользователя (смарт-карта, USB-токен, программный эмулятор токена на дискете или жестком диске) в формате PKCS#7.

Таким образом, принцип централизованного управления безопасностью корпоративной системы на базе политик ГПБ и ЛПБ позволяет формировать целостную и непротиворечивую политику безопасности компании, независимую от форматов и содержания настроек отдельных средств защиты, реализующих данную политику. Для этого используется патентованная технология TrustWorks, которая позволяет интерпретировать правила безопасности ГПБ и ставить их в соответствие с топологией защищаемой сети, автоматически вычислять и предоставлять локальные политики безопасности всем узлам, где реализуется заданная политика безопасности корпоративной системы.

11.4.2. Продукты компании Cisco для управления безопасностью сетей

Компания Cisco Systems, признанный лидер в области сетевых решений, предлагает также широкий выбор продуктов в области обеспечения информационной безопасности - от межсетевых экранов и систем предотвращения атак до средств персональной защиты рабочих станций и систем централизованного управления средствами защиты [21].

Система управления Cisco Security Manager. Cisco Security Manager (CSM) - система централизованного управления всеми средствами защиты компании Cisco, пришедшая на смену CiscoWorks VMS. Отличительными особенностями CSM являются поддержка большего числа устройств защиты, различные формы представления информации, механизмы обнаружения несоответствий в политике безопасности, автоматизация рутинных задач и т.д.

Основные возможности GSM:

- графический интерфейс управления;
- различные формы представления информации - в виде топологии сети, географической карты, таблицы правил;
- обнаружение конфликтов в правилах политики безопасности;
- обнаружение правил, не влияющих на защищенность сети;
- группирование объектов;
- «клонирование» настроек для ускорения внедрения средств защиты;
- поддержка иерархии и наследования политик безопасности;
- откат к предыдущей конфигурации;
- импорт настроек из различных источников;
- инвентаризация политик для уже внедренных средств защиты;
- автоматическая настройка VPN-туннелей для различных топологий (Site-to-Site, Hub & Spoke, Partial Mesh, Full Mesh и т.д.);
- управление механизмами отказоустойчивости, балансировки нагрузки и контроля качества обслуживания для управляемых средств защиты;
- ролевое управление административным доступом с помощью Cisco Secure ACS;
- автоматическое обновление средств защиты;
- управление ACL и VLAN на Catalyst 6500 и Cisco 7600;
- интеграция с Cisco MARS для корреляции сетевых событий и заданных правил на МЭ, что помогает более быстро принимать решения и повышает работоспособность сети;
- управление и конфигурирование политик безопасности на МСЭ Cisco, включая устройства Cisco ASA 5500, Cisco PIX, модули на Cisco Catalyst 6500;
- обеспечение высокой доступности;
- контроль административных действий на защитных устройствах;
- управление SSL VPN.

Программно-аппаратный комплекс Cisco MARS. Программно-аппаратный комплекс Cisco Monitoring, Analysis and Response System (MARS) предназначен для управления противодействием угрозам безопасности. В качестве источников информации о них могут выступать: сетевое оборудование (маршрутизаторы и коммутаторы), средства защиты (межсетевые экраны, антивирусы, системы обнаружения атак и сканеры безопасности), журналы регистрации ОС (Solaris, Windows NT, 2000, 2003, Linux) и приложений (СУБД, web и т.д.), а также сетевой трафик (например, Cisco Netflow). Cisco MARS поддерживает решения различных производителей - Cisco, ISS, Check Point, Symantec, NetScreen, Extreme,

Snort, McAfee, eEye, Oracle, Microsoft и т.д. Механизм ContextCorrelationTM позволяет проанализировать и сопоставить события от разнородных средств защиты.

Визуализация их на карте сети в реальном времени достигается с помощью механизма SureVectorTM. Данные механизмы позволяют отобразить путь распространения атаки в режиме реального времени. Автоматическое блокирование обнаруженных атак достигается с помощью механизма AutoMitigateTM, который позволяет реконфигурировать различные средства защиты и сетевое оборудование.

Основные возможности MARS:

- обработка до 10 000 событий в секунду или свыше 300 000 событий Netflow в секунду;
- возможность создания собственных правил корреляции;
- уведомление об обнаруженных проблемах по e-mail, SNMP, через syslog и на пейджер;
- визуализация атаки на канальном и сетевом уровнях;
- поддержка Syslog, SNMP, RDEP, SDEE, NetFlow, системных и пользовательских журналов регистрации в качестве источников информации;
- возможность подключения собственных средств защиты для анализа;
- эффективное отсечение ложных срабатываний и шума, а также обнаружение атак, пропущенных отдельными средствами защиты;
- обнаружение аномалий с помощью протокола NetFlow;
- создание и автоматическое обновление карты сети, включая импорт из CiscoWorks и других систем сетевого управления;
- поддержка IOS 802.1x, NAC (фаза 2);
- мониторинг механизмов защиты коммутаторов (Dynamic ARP Inspection, IP Source Guard и т.д.);
- интеграция с Cisco Security Manager (CSM Policy Lookup);
- интеграция с системами управления инцидентами с помощью XML Incident Notification;
- слежение за состоянием контролируемых устройств;
- интеграция с Cisco Incident Control System (ICS);
- аутентификация на RADIUS-сервере;
- мониторинг работоспособности компонентов Cisco MARS;
- syslog forwarding;
- динамическое распознавание новых сигнатур атак на Cisco IPS и загрузка их в Cisco MARS.

Cisco IP Solution Center. Cisco IP Solution Center (ISC) - платформа централизованного управления сетевой инфраструктурой крупных компаний и сервис-провайдеров. В том числе ISC управляет и решениями по информационной безопасности - механизмами построения VPN (ЛВС - ЛВС, удаленный доступ, EasyVPN, DMVPN), межсетевыми экранами, сетевой трансляцией адресов (NAT) и качеством сервиса (QoS) на маршрутизаторах с Cisco IOS, МСЭ Cisco Pix и устройствах VPN Concentrator. Эту задачу решает специальное приложение - ISC Security Management.

ISC Security Management предоставляет возможность управления жизненным циклом средств защиты, начиная от создания политик безопасности, активации и аудита защитной услуги и заканчивая оценкой качества предоставления защитной услуги и реконфигурацией используемой политики. Все это позволяет обеспечивать безопасность инфраструктуры без нарушения ее доступности и устойчивости.

11.4.3. Продукты компании IBM для управления средствами безопасности

Управление безопасностью имеет много аспектов, и только при комплексном подходе к решению этой задачи можно создать действительно безопасную среду функционирования ИС предприятия. Два подразделения IBM Tivoli и IBM Internet Security Systems (IBM ISS) компании IBM предлагают средства защиты и управления для обеспечения безопасности ИТ-инфраструктуры предприятий.

Продукты IBM Tivoli для управления средствами безопасности. На рис.11.5 представлена информация о функциональности продуктов IBM Tivoli для обеспечения безопасности КИС [20].

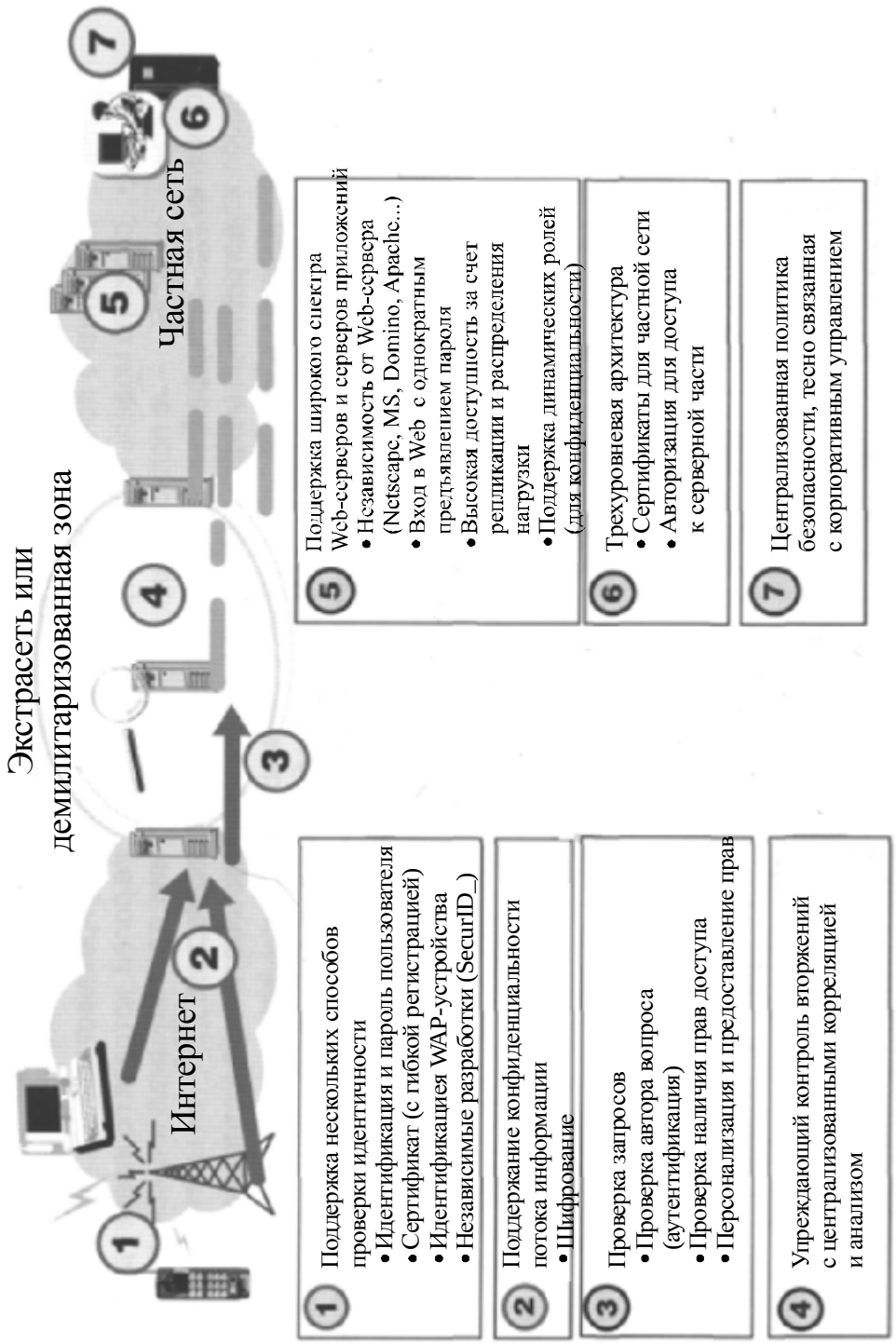

Рис.11.5. Функциональность продуктов IBM Tivoli для обеспечения безопасности КИС

При формировании стратегии безопасности предприятия подразделение IBM Tivoli выделяет в качестве приоритетных задач:

- выработку политики доступа к ресурсам или данным и реализация ее на всех уровнях корпоративной инфраструктуры;
- комплексную защиту от несанкционированного проникновения в сеть, вирусных атак и других угроз вторжения извне и изнутри.

Для решения этих проблем обеспечения безопасности в продуктах IBM Tivoli предусмотрена реализация нескольких функций. Первая функция - *управление идентификацией* (Identity Management) - включает управление процессами аутентификации и авторизации пользователей по отношению к информационным ресурсам предприятия. Вторая функция - *управление доступом* (Access Management) к

информационным ресурсам предприятия. Третья функция - *централизованное управление и реагирование на различные угрозы и попытки вторжения, направленные на информационные ресурсы предприятия (Security Operations Manager).* Функция дает возможность определять вторжение извне и изнутри и автоматически запускать превентивные процедуры. Четвертая функция - *создание вычислительной и коммуникационной основы* (Management Framework) для функционирования всех модулей обеспечения безопасности.

Для реализации перечисленных функций подразделение IBM Tivoli предлагает следующие продукты:

- IBM Tivoli Identity Manager;
- IBM Tivoli Access Manager;
- IBM Tivoli Security Operations Manager;
- IBM Tivoli Management Framework и др.

IBM Tivoli Identity Manager представляет собой *автоматизированное, защищенное и основанное на политиках решение по управлению пользователями*. IBM Tivoli Identity Manager предоставляет:

- интуитивно понятный Web-интерфейс администрирования;
- сложную модель администрирования на основе ролей, которая позволяет делегировать административные полномочия;
- Web-интерфейсы самообслуживания и запросов/ответов;
- встроенный механизм документооборота для автоматической отправки пользовательских запросов на утверждение, а утвержденных запросов - на выполнение;
- встроенный механизм автоматизации выполнения административных запросов;
- набор инструментов для управления приложениями.

Используя интерфейс самообслуживания и интерфейс делегирования администраторских полномочий на основе ролей, администратор может объединять пользователей в группы в соответствии с потребностями бизнеса и при необходимости делегировать определенные функции управления (право добавлять, удалять, модифицировать, просматривать учетные записи пользователей и сбрасывать пароли) другим организациям и подразделениям. Помощники администраторов, облеченные теми или иными полномочиями, благодаря политикам на основе задач могут видеть только то, к чему им предоставлен доступ.

IBM Tivoli Access Manager for e-business - это универсальное решение для управления доступом на основе политик, предназначенное для электронного бизнеса и корпоративных приложений. Tivoli Access Manager for e-business позволяет организациям управлять как проводным, так и беспроводным доступом к приложениям и данным, обеспечивая возможность единого входа в систему (SSO) для авторизованных пользователей. Это решение обеспечивает комплексную безопасность, в том числе персональную Web-регистрацию, распределенное Web-администрирование и безопасность с учетом политик.

IBM Tivoli Access Manager for Enterprise Single Sign-On (TAME-SSO) обеспечивает строгую ***одношаговую*** аутентификацию, позволяющую пользователям применять один пароль для входа во все необходимые им приложения, включая корпоративные приложения и приложения в Интернет. TAM E-SSO позволяет осуществлять регистрацию с помощью одного пароля практически для любого Windows, Web- или разработанного внутри компании приложения. TAM E-SSO использует приложение-агент, устанавливаемое на ПК пользователя, которое отвечает на запросы приложения (на ввод идентификационных данных пользователя) от имени пользователя. Агент автоматически предоставляет приложению все данные, необходимые для аутентификации пользователя, включая имя пользователя, пароль или другие данные, требуемые приложением. TAM E-SSO повышает безопасность за счет широкого выбора факторов строгой аутентификации и обеспечивает ведение отчетности о соответствии требованиям всех приложений в пределах предприятия.

Программные продукты ***IBM Tivoli Security Operations Manager (TSOM)*** и ***IBM Tivoli Compliance Insight Manager (TCIM)*** позволяют *централизованно управлять и реагировать на различные угрозы* и попытки вторжения, направленные на информационные ресурсы предприятия. Эти продукты обладают следующими возможностями.

IBM Tivoli Security Operations Manager (TSOM) - это ***платформа для повышения эффективности и прозрачности действий по обеспечению безопасности и управлению информационными рисками.*** TSOM обеспечивает оперативный мониторинг событий безопасности и предназначен в основном для снижения рисков и угроз, исходящих от внешних нарушителей и технологий. TSOM представляет собой набор программных модулей для построения системы сбора и корреляции сообщений от различных устройств и программ обеспечения информационной безопасности. TSOM предназначен для служб эксплуатации систем информационной безопасности.

IBM Tivoli Compliance Insight Manager (TCIM) осуществляет контроль преимущественно за внутренними угрозами, исходящими от пользователей, в том числе с высокими полномочиями доступа (администраторы сетей, баз данных, ОС, приложений). TCIM обеспечивает корреляцию событий безопасности от различных источников: операционных систем, СУБД, приложений, сетевых устройств, средств безопасности, мэйнфреймов, приведение полученных больших объемов информации о событиях безопасности к удобному для восприятию виду (КТО, ЧТО, ГДЕ, КОГДА, ОТКУДА, КУДА), возможности расследования инцидентов, контроль за действиями внутренних пользователей, сторонних консультантов, контроль соответствия нормативным требованиям (включая ISO 27001, ISO 17799 и др.).

IBM Tivoli Management Framework создает вычислительную и коммуникационную основу для функционирования всех модулей Tivoli, обеспечивая тесную интеграцию компонентов Tivoli, стандартные интерфейсы, средства для расширения функциональности, кросс-платформность и возможность включения собственных приложений в единую систему управления. Содержащийся в Tivoli Framework управляющий агент обслуживает все остальные модули Tivoli. Этот агент устанавливается на компьютер один раз, так что при добавлении новой функциональности необходимо установить только серверную часть соответствующего модуля. После этого новые функции управления будут доступны на всех компьютерах с управляющим агентом Tivoli.

Программные средства превентивной защиты подразделения IBM ISS. Подразделение IBM Internet Security Systems (IBM ISS) предлагает средства превентивной защиты для обеспечения безопасности ИТ-инфраструктуры предприятия. Эти средства превентивной защиты тесно интегрированы с существующими бизнес-процессами предприятия и предназначены для комплексного укрепления всей инфраструктуры - от шлюза до ядра сети, от центра до самых удаленных точек.

Ведущую роль среди средств превентивной защиты играет семейство продуктов IBM Proventia. Это мощная интегрированная платформа для защиты сети, рабочих станций и серверов, в которую включены средства антивирусной защиты, брандмауэр, виртуальные частные сети (VPN), средства обнаружения и предотвращения сетевых атак, средства обеспечения безопасности приложений, средства защиты от спама, средства фильтрации контента и единый центр управления этими средствами защиты IBM Proventia Management SiteProtector.

Система управления безопасностью IBM Proventia Management SiteProtector. Система централизованного управления IBM Proventia Management SiteProtector выпускается в виде программного комплекса и в виде программно-аппаратного устройства. Система управления SiteProtector решает следующие основные задачи:

- *управление средствами защиты* - SiteProtector позволяет управлять всем спектром продуктов IBM ISS. Помимо этого, имеется возможность управления средствами защиты информации третьих фирм (Third Party), включая межсетевые экраны, средства построения VPN и т.д.
- *сбор и отображение событий в реальном режиме времени* - каждое устройство семейства Proventia или агент системы защиты сообщает системе SiteProtector обо всех детектируемых событиях. Кроме того, могут быть подключены системы защиты третьих фирм (Third Party). По каждому из зафиксированных событий предоставляется подробная информация.
- *фильтрация событий на консоли управления* - в системе SiteProtector используются фильтры событий для сокращения массы данных, отображаемых на консоли. На этапе анализа событий используется модуль корреляции данных Security Fusion. Предопределенные фильтры позволяют быстро выяснить следующие данные:

- кто атакует выбранные ресурсы,
- какие ресурсы являются источниками атак,
- какие узлы уязвимы,
- какие узлы атакуют,
- какие уязвимости на выбранных ресурсах,
- какие атаки нанесли ущерб;

- *автоматическое обновление компонентов средств защиты (X-Press Update)* - в системе SiteProtector реализован механизм X-Press Update, который позволит автоматически и своевременно получать обновления базы данных уязвимостей и атак из специального хранилища по каналу, защищенному от несанкционированного доступа.
- *система генерации отчетов* - SiteProtector включает в себя множество предустановленных категорий отчетов. Отчеты могут отображаться как в графическом, так и в текстовом виде.

Основные достоинства SiteProtector:

- *система управления на аппаратной платформе* - возможность приобретения устройства с предустановленным программным обеспечением (SiteProtector Management Appliance SP1001);
- *работа с ролями и правами доступа* - в SiteProtector реализованы механизмы объединения пользователей в группы и составления модели полномочий пользователей. Благодаря модели полномочий механизм создания и сопровождения групп пользователей приобретает большую гибкость и эластичность;
- *поддержка отказоустойчивой конфигурации* - модуль SecureSync реализует механизм отказоустойчивой конфигурации для системы управления SiteProtector.

Вопросы для самоконтроля

1. Назовите задачи системы управления информационной безопасностью КИС.
2. Как осуществляется управление учетными записями и правами доступа к рабочим станциям, серверам и другим активным устройствам КИС?
3. В чем суть концепции глобального управления безопасностью GSM (Global Security Management)?
4. Объясните понятия «глобальная и локальная политики безопасности».

5. Опишите функционирование системы управления информационной безопасностью GSM.

6. Как осуществляется защита ресурсов в системе управления информационной безопасностью GSM?

7. Как осуществляется управление средствами информационной безопасности масштаба предприятия в системе GSM?

8. Опишите централизованное управление безопасностью, реализованное в продуктах Застава.

9. Опишите возможности системы управления Cisco Security Manager и программно-аппаратного комплекса управления Cisco MARS.

10. Какие функции реализуют продукты IBM Tivoli для обеспечения информационной безопасности КИС?

11. Назовите основные продукты IBM Tivoli и опишите их возможности.

12. Какие задачи решает система управления безопасностью IBM Proventia Management SiteProtector?

Глава 12. Стандарты информационной безопасности

Иногда знание общих законов способно
заменить незнание конкретных фактов.
Гельвеций

Проблемой информационной компьютерной безопасности начали заниматься с того самого момента, когда компьютер стал обрабатывать данные, ценность которых высока для пользователя. В последние годы в связи с ростом спроса на электронные услуги и развитием компьютерных систем и сетей ситуация в сфере информационной безопасности серьезно обострилась, а вопрос стандартизации подходов к ее решению стал особенно актуальным как для разработчиков, так и для пользователей ИТ-средств.

12.1. Роль стандартов информационной безопасности

Главная задача стандартов информационной безопасности - создать основу для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности.

Потребители заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности. Потребители также нуждаются в инструменте, с помощью которого они могли бы формулировать свои требования производителям. При этом потребителей интересуют исключительно характеристики и свойства конечного продукта, а не методы и средства их достижения. К сожалению, многие потребители не понимают, что требования безопасности обязательно противоречат функциональным требованиям (удобству работы, быстродействию и т.д.), налагают ограничения на совместимость и, как правило, вынуждают отказаться от широко распространенных и поэтому незащищенных прикладных программных средств.

Производители нуждаются в стандартах как средстве сравнения возможностей своих продуктов и в применении процедуры сертификации как механизма объективной оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора. С точки зрения производителя, требования должны быть максимально конкретными и регламентировать необходимость применения тех или иных средств, механизмов, алгоритмов и т.д. Кроме того, требования не должны противоречить существующим парадигмам обработки информации, архитектуре вычислительных систем и технологиям создания информационных продуктов. Этот подход также нельзя признать в качестве доминирующего, так как он не учитывает нужд пользователей и пытается подогнать требования защиты под существующие системы и технологии.

Эксперты по квалификации и *специалисты по сертификации* рассматривают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый продуктами информационных технологий, и предоставить потребителям возможность сделать обоснованный выбор. Эксперты по квалификации находятся в двойственном положении: с одной стороны, они, а также производители заинтересованы в четких и простых критериях, над которыми не надо ломать голову как их применить к конкретному продукту, а с другой стороны, они должны дать обоснованный ответ пользователям - удовлетворяет продукт их нужды или нет. Таким образом, перед стандартами информационной безопасности стоит непростая задача - примирить три разные точки зрения и создать эффективный механизм взаимодействия всех сторон. Причем ущемление потребностей хотя бы одной из них приведет к невозможности взаимопонимания и взаимодействия и, следовательно, не позволит решить общую задачу - создание защищенной системы обработки информации.

Необходимость в таких стандартах была осознана достаточно давно, и в этом направлении достигнут существенный прогресс, закрепленный в документах разработки 1990-х годов. Первым и наиболее известным документом была *Оранжевая книга* (по цвету обложки) «Критерии безопасности компьютерных систем» Министерства обороны США. В этом документе определены четыре уровня *безопасности* - *D*, *C*, *B* и *A*. По мере перехода от уровня *D* до *A* к надежности систем предъявляются все более жесткие требования. Уровни *C* и *B* подразделяются на *классы* (*C*1, *C*2, *B*1, *B*2, *B*3). Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому *классу*, ее защита должна удовлетворять оговоренным требованиям. К другим важным стандартам информационной безопасности этого поколения относятся «Руководящие документы Гостехкомиссии России», «Европейские критерии безопасности информационных технологий», «Федеральные критерии безопасности информационных технологий США», «Канадские критерии безопасности компьютерных систем» [11, 12].

В последнее время в разных странах появилось новое поколение стандартов в области защиты информации, посвященных практическим вопросам управления информационной безопасностью компании.

Это, прежде всего, международные стандарты управления информационной безопасностью ISO 15408, ISO 17799 и некоторые другие. Представляется целесообразным проанализировать наиболее важные из этих документов, сопоставить содержащиеся в них требования и критерии, а также оценить эффективность их практического применения.

12.2. Международные стандарты информационной безопасности

В соответствии с международными и национальными стандартами обеспечение информационной безопасности в любой компании предполагает следующее:

- определение целей обеспечения информационной безопасности компьютерных систем;
- создание эффективной системы управления информационной безопасностью;
- расчет совокупности детализированных качественных и количественных показателей для оценки соответствия информационной безопасности поставленным целям;
- применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
- использование методик управления безопасностью, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Рассмотрим наиболее известные международные стандарты в области защиты информации, которые могут быть использованы в отечественных условиях [1, 5].

12.2.1. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)

В настоящее время Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью - Информационные технологии (Information technology - Information security management)» является одним из наиболее известных стандартов в области защиты информации. Данный стандарт был разработан на основе первой части Британского стандарта BS 7799-1:1995 «Практические рекомендации по управлению информационной безопасностью (Information security management - Part 1: Code of practice for information security management)» и относится к новому поколению стандартов информационной безопасности компьютерных информационных систем.

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;
- классификация и управление корпоративными информационными ресурсами;
- кадровый менеджмент и информационная безопасность;
- физическая безопасность;
- администрирование безопасности корпоративных информационных систем;
- управление доступом;
- требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения;
- управление бизнес-процессами компании с точки зрения информационной безопасности;
- внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799-2:2000 «Спецификации систем управления информационной безопасностью (Information security management - Part 2: Specification for information security management systems)» определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов - British Standards Institution (BSI), изданные в период 1995 - 2003 гг. в виде следующей серии:

- Введение в проблему управления информационной безопасности (Information security managment: an introduction);
- Возможности сертификации на требования стандарта BS 7799 (Preparing for BS 7799 sertification);
- Руководство BS 7799 по оценке и управлению рисками (Guide to BS 7799 risk assessment and risk management);
- Руководство для проведения аудита на требования стандарта (BS 7799Guide to BS 7799 auditing);

- Практические рекомендации по управлению безопасностью информационных технологий (Code of practice for IT management).

В 2002 году Международный стандарт ISO 17799 (BS7799) был пересмотрен и существенно дополнен. В новом варианте этого стандарта большое внимание уделено вопросам повышения культуры защиты информации в различных международных компаниях, в том числе вопросам обучения и изначальной интеграции процедур и механизмов оценки и управления информационной безопасностью в информационные технологии корпоративных систем. По мнению специалистов, обновление Международного стандарта ISO 17799 (BS7799) позволит не только повысить культуру защиты информационных активов компании, но и скоординировать действия различных ведущих государственных и коммерческих структур в области защиты информации.

12.2.2. Германский стандарт BSI

В отличие от ISO 17799, германское Руководство по защите информационных технологий для базового уровня защищенности посвящено детальному рассмотрению частных вопросов управления информационной безопасностью компании.

В германском стандарте BSI представлены:

- общая методика управления информационной безопасностью (организация менеджмента в области информационной безопасности, методология использования руководства);
- описания компонентов современных информационных технологий;
- описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса);
- характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны);
- характеристики основных информационных активов компании (в том числе аппаратное и программное обеспечение, например рабочие станции и серверы под управлением операционных систем семейства DOS, Windows и UNIX);
- характеристики компьютерных сетей на основе различных сетевых технологий, например сети Novell NetWare, сети UNIX и Windows;
- характеристика активного и пассивного телекоммуникационного оборудования ведущих поставщиков, например Cisco Systems;
- подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).

Вопросы защиты приведенных информационных активов компании рассматриваются по определенному сценарию: общее описание информационного актива компании - возможные угрозы и уязвимости безопасности - возможные меры и средства контроля и защиты.

12.2.3. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»

Одним из главных результатов стандартизации в сфере систематизации требований и характеристик защищенных информационных комплексов стала система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных документов. Важное место в этой системе стандартов занимает стандарт ISO 15408 известный как «Common Criteria».

В 1990 году Международная организация по стандартизации (ISO) приступила к разработке международного стандарта по критериям оценки безопасности информационных технологий для общего использования «Common Criteria», или «Общие критерии безопасности информационных технологий».

В разработке «Общих критериев» участвовали: Национальный институт стандартов и технологии и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Голландия), органы исполнения Программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция), которые опирались на свой солидный задел.

«Общие критерии» обобщили содержание и опыт использования Оранжевой книги, развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США.

За десятилетие разработки лучшими специалистами мира «Общие критерии» неоднократно редактировались. В результате был подготовлен Международный стандарт ISO/IEC 15408.

Первые две версии «Общих критериев» были опубликованы соответственно в январе и мае 1998 года. Версия 2.1 этого стандарта утверждена 8 июня 1999 года Международной организацией по стандартизации (ISO) в качестве международного стандарта информационной безопасности ISO/IEC 15408 под названием «Общие критерии оценки безопасности информационных технологий» (ОК).

В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК - полнота требований безопасности

и их систематизация, гибкость в применении и открытость для последующего развития. ОК адаптированы к потребностям взаимного признания результатов оценки безопасности ИТ в мировом масштабе и предназначены для использования в качестве основы для такой оценки. Они позволяют сравнить результаты независимых оценок информационной безопасности и допустимых рисков на основе множества общих требований к функциям безопасности средств и систем ИТ, а также гарантий, применяемых к ним в процессе тестирования.

Основываясь на общем перечне (наборе) требований, в процессе выработки оценки уровня защиты устанавливается уровень доверия. Результаты оценок защиты позволяют определить для компании достаточность защиты корпоративной информационной системы.

Ведущие мировые производители оборудования ИТ основательно подготовились к этому моменту и сразу стали поставлять заказчикам средства, полностью отвечающие требованиям ОК.

Принятый базовый стандарт информационной безопасности ISO 15408, безусловно, очень важен для российских разработчиков.

ОК разрабатывались в расчете на то, чтобы удовлетворить запросы трех групп специалистов, в равной степени являющихся пользователями этого документа: производителей и потребителей продуктов информационных технологий, а также экспертов по оценке уровня их безопасности. ОК обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

ОК рассматривают информационную безопасность, во-первых, как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ-продуктом, а также доступности ресурсов ВС, и, во-вторых, ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации. Поэтому в концепцию ОК входят все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности.

Потребители ИТ-продуктов озабочены наличием угроз безопасности, приводящих к определенным рискам для обрабатываемой информации. Для противодействия этим угрозам ИТ-продукты должны включать в свой состав средства защиты, противодействующие этим угрозам и направленные на устранение уязвимостей, однако ошибки в средствах защиты, в свою очередь, могут приводить к появлению новых уязвимостей. Сертификация средств защиты позволяет подтвердить их адекватность угрозам и рискам.

ОК регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов, ОК предлагают концепцию процесса разработки и квалификационного анализа ИТ-продуктов, требующую от потребителей и производителей большой работы по составлению и оформлению довольно объемных и подробных нормативных документов. Требования ОК являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности информационных технологий.

Стандарт ISO 15408 поднял стандартизацию информационных технологий на межгосударственный уровень. Возникла реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных информационных систем, а это откроет новые сферы применения информационных технологий.

Некоторые особенности стандарта ISO 15408 приведены в разделе 12.3, где рассматривается стандарт ГОСТ Р ИСО/МЭК 15408, являющийся аналогом стандарта ISO 15408.

12.2.4. Стандарты для беспроводных сетей

Стандарт IEEE 802.11. В 1990 году Комитет IEEE 802 сформировал рабочую группу 802.11 для разработки стандарта для беспроводных локальных сетей. Работы по созданию стандарта были завершены через 7 лет. В 1997 году была ратифицирована первая спецификация беспроводного стандарта IEEE 802.11, обеспечивающего передачу данных с гарантированной скоростью 1 Мб/с (в некоторых случаях до 2 Мб/с) в полосе частот 2,4 ГГц. Эта полоса частот доступна для нелицензионного использования в большинстве стран мира.

Стандарт IEEE 802.11 является базовым стандартом и определяет протоколы, необходимые для организации беспроводных локальных сетей WLAN (Wireless Local Area Network). Основные из них - протокол управления доступом к среде MAC (Medium Accsess Control - нижний подуровень канального уровня) и протокол PHY передачи сигналов в физической среде. В качестве физической среды допускается использование радиоволн и инфракрасного излучения.

В основу стандарта IEEE 802.11 положена сотовая архитектура, причем сеть может состоять как из одной, так и нескольких ячеек. Каждая сота управляется базовой станцией, называемой *точкой доступа* AP (Access Point), которая вместе с находящимися в пределах радиуса ее действия рабочими станциями пользователей образует *базовую зону обслуживания* BSS (Basic Service Set). Точки доступа многосотовой сети взаимодействуют между собой через *распределительную систему* DS (Distribution System), представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему, образует *расширенную зону обслуживания* ESS

(Extended Service Set). Стандартом предусмотрен также односотовый вариант беспроводной сети, который может быть реализован и без точки доступа, при этом часть ее функций выполняются непосредственно рабочими станциями.

Для обеспечения перехода мобильных рабочих станций из зоны действия одной точки доступа к другой в многосотовых системах предусмотрены специальные процедуры сканирования (активного и пассивного прослушивания эфира) и присоединения (Association), однако строгих спецификаций по реализации роуминга стандарт 802.11 не предусматривает.

Для защиты WLAN стандартом IEEE 802.11 предусмотрен алгоритм WEP (Wired Equivalent Privacy). Он включает средства противодействия несанкционированному доступу к сети, а также шифрование для предотвращения перехвата информации.

Однако заложенная в первую спецификацию стандарта IEEE 802.11 скорость передачи данных в беспроводной сети уже не удовлетворяла потребностям пользователей. Алгоритм WEP страдал рядом существенных недостатков - отсутствие управления ключом, использование общего статического ключа, малые разрядности ключа и вектора инициализации, сложности использования алгоритма RC4.

Чтобы сделать технологию Wireless LAN недорогой, популярной и удовлетворяющей жестким требованиям бизнес-приложений, разработчики были вынуждены создать семейство новых спецификаций стандарта IEEE 802.11 a, b,.., i. Стандарты этого семейства, по сути, являются беспроводными расширениями протокола Ethernet, что обеспечивает хорошее взаимодействие с проводными сетями Ethernet.

Стандарт IEEE 802.11b. Этот стандарт применяется наиболее широко из всех стандартов 802.11. Высокоскоростной стандарт 802.11b был ратифицирован IEEE в сентябре 1999 года как развитие базового стандарта 802.11; в стандарте 802.11b используется полоса частот 2,4 ГГц, скорость передачи достигает 11 Мб/с (подобно Ethernet). Благодаря ориентации на освоенный диапазон 2,4 ГГц стандарт 802.11b завоевал большую популярность у производителей оборудования. В качестве базовой радиотехнологии в нем используется метод распределенного спектра с прямой последовательностью DSSS (Direct Sequence Spread Spectrum), который отличается высокой устойчивостью к искажению данных помехами, в том числе преднамеренными. Этот стандарт получил широкое распространение, и беспроводные LAN стали привлекательным решением с технической и финансовой точки зрения.

Для простоты запоминания в качестве общего имени для стандартов 802.11b и 802.11a, а также всех последующих, относящихся к беспроводным локальным сетям (WLAN), был введен термин Wi-Fi (Wireless Fidelity). Этот термин введен Ассоциацией беспроводной совместимости с Ethernet WECA (Wireless Ethernet Compatibility Aliance). Если устройство помечено этим знаком, оно протестировано на совместимость с другими устройствами 802.11.

Стандарт IEEE 802.11a. Стандарт предназначен для работы в частотном диапазоне 5 ГГц. Скорость передачи данных до 54 Мбит/с, т.е. примерно в пять раз быстрее сетей 802.11b. Ассоциация WECA называет этот стандарт WiFi5. Это наиболее широкополосный из семейства стандартов 802.11. Определены три обязательные скорости - 6, 12 и 24 Мбит/с и пять необязательных - 9, 18, 36, 48 и 54 Мбит/с. В качестве метода модуляции сигнала принято ортогональное частотное мультиплексирование OFDM (Orthogonal Frequency Division Multiplexing). Его отличие от метода DSSS заключается в том, что OFDM предполагает параллельную передачу полезного сигнала одновременно по нескольким частотам диапазона, в то время как технологии расширения спектра DSSS передают сигналы последовательно. В результате повышается пропускная способность канала и качество сигнала. К недостаткам стандарта 802.11a относятся большая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия (около 100 м).

Стандарт IEEE 802.11g. Стандарт представляет собой развитие стандарта 802.11b и обратно совместим с 802.11b. Предназначен для обеспечения скоростей передачи данных до 54 Мбит/с. В числе достоинств 802.11g надо отметить низкую потребляемую мощность, большие расстояния (до 300 м) и высокую проникающую способность сигнала.

Стандарт IEEE 802.11i. В 2004 году IEEE ратифицировал стандарт обеспечения безопасности в беспроводных сетях IEEE 802.11i. Этот стандарт решил существовавшие проблемы в области аутентификации и протокола шифрования, обеспечив значительно более высокий уровень безопасности. Стандарт 802.11i может применяться в сетях Wi-Fi независимо от используемого стандарта 802.11a, b или g.

В настоящее время существуют два очень похожих стандарта - WPA и 802.11i. Они оба используют механизм 802.1x для обеспечения надежной аутентификации, сильные алгоритмы шифрования и предназначены для замены протокола WEP.

WPA был разработан в Wi-Fi Alliance как решение, которое можно применить немедленно, не дожидаясь завершения длительной процедуры ратификации 802.11i в IEEE.

Основное отличие двух стандартов заключается в использовании различных механизмов шифрования. В WPA применяется протокол TKIP (Temporal Key Integrity Protocol), который, так же как и WEP, использует шифр RC4, но значительно более безопасным способом. Обеспечение конфиденциальности данных в стандарте IEEE 802.11i основано на использовании алгоритма шифрования AES (Advanced Encryption Standard). Использующий его защитный протокол получил название CCMP (Counter-Mode CBC MAC Protocol). Алгоритм AES обладает высокой криптостойкостью. Длина ключа AES равна 128, 192 или 256 бит, что обеспечивает наиболее надежное шифрование из доступных сейчас.

Стандарт 802.11i предполагает наличие трех участников процесса аутентификации. Это сервер аутентификации AS (Authentication Server), точка доступа AP (Access Point) и рабочая станция STA (Station). В процессе шифрования данных участвуют только AP и STA (AS не используется). Стандарт предусматривает двустороннюю аутентификацию (в отличие от WEP, где аутентифицируется только рабочая станция, но не точка доступа). При этом местами принятия решения о разрешении доступа являются сервер аутентификации AS и рабочая станция STA, а местами исполнения этого решения - точка доступа AP и STA.

Для работы по стандарту 802.11i создается иерархия ключей, включающая мастер-ключ MK (Master Key), парный мастер-ключ PMK (Pairwise Master Key), парный временный ключ PTK (Pairwise Transient Key), а также групповые временные ключи GTK (Group Transient Key), служащие для защиты широковещательного сетевого трафика.

MK - это симметричный ключ, реализующий решение STA и AS о взаимной аутентификации. Для каждой сессии создается новый MK.

PMK - обновляемый симметричный ключ, владение которым означает разрешение (авторизацию) на доступ к среде передачи данных в течение данной сессии. PMK создается на основе MK. Для каждой пары STA и AP в каждой сессии создается новый PMK.

PTK - это коллекция операционных ключей, которые используются для привязки PMK к данным STA и AP, для распространения GTK и шифрования данных.

Процесс аутентификации и доставки ключей определяется стандартом 802.1x. Он предоставляет возможность использовать в беспроводных сетях такие традиционные серверы аутентификации, как RADIUS (Remote Authentication Dial-In User Server). Стандарт 802.11i не определяет тип сервера аутентификации, но использование RADIUS для этой цели является стандартным решением.

Транспортом для сообщений 802.1x служит протокол EAP (Extensible Authentication Protocol). EAP позволяет легко добавлять новые методы аутентификации. Точке доступа не требуется знать об используемом методе аутентификации, поэтому изменение метода никак не затрагивает точку доступа.

Наиболее популярные методы EAP - это LEAP, PEAP, TTLS и FAST. Каждый из методов имеет свои сильные и слабые стороны, условия применения, по-разному поддерживается производителями оборудования и программного обеспечения.

Можно выделить пять фаз работы 802.11i. *Первая фаза* - обнаружение. В этой фазе рабочая станция STA находит точку доступа AP, с которой может установить связь, и получает от нее используемые в данной сети параметры безопасности. Таким образом STA узнает идентификатор сети SSID и методы аутентификации, доступные в данной сети. Затем STA выбирает метод аутентификации и между STA и AP устанавливается соединение. После этого STA и AP готовы к началу второй фазы. *Вторая фаза* - аутентификация. В этой фазе выполняется взаимная аутентификация STA и сервера AS, создаются MK и PMK. В данной фазе STA и AP блокируют весь трафик, кроме трафика 802.1x. В *третьей фазе* AS перемещает ключ PMK на AP. Теперь STA и AP владеют действительными ключами PMK. *Четвертая фаза* - управление ключами 802.1x. В этой фазе происходит генерация, привязка и верификация ключа PTK. *Пятая фаза* - шифрование и передача данных. Для шифрования используется соответствующая часть PTK.

Стандартом 802.11i предусмотрен режим PSK (Pre-Shared Key), который позволяет обойтись без сервера аутентификации AS. При использовании этого режима на STA и на AP вручную вводится Pre-Shared Key, который используется в качестве PMK. Дальше генерация PTK происходит описанным выше порядком. Режим PSK может использоваться в небольших сетях, где нецелесообразно устанавливать сервер AS.

12.2.5. Стандарты информационной безопасности для Интернета

В последнее время в мире бурно развивается электронная коммерция посредством сети Интернет, что в основном определяется прогрессом в области безопасности информации. При этом базовыми задачами являются обеспечение доступности, конфиденциальности, целостности и юридической значимости информации.

По оценке Комитета ООН по предупреждению преступности и борьбе с ней, компьютерная преступность вышла на уровень одной из международных проблем. Поэтому чрезвычайно важно добиваться эффективного решения проблем обеспечения безопасности коммерческой информации в глобальной сети Интернет и смежных интранет-сетях, которые по своей технической сущности не имеют принципиальных отличий и различаются в основном масштабами и открытостью.

Рассмотрим особенности стандартизации процесса обеспечения безопасности коммерческой информации в сетях с протоколом передачи данных IP/TCP и с акцентом на защиту телекоммуникаций [26].

Обеспечение безопасности ИТ особенно актуально для открытых систем коммерческого применения, обрабатывающих информацию ограниченного доступа, не содержащую государственную тайну. Под открытыми системами понимают совокупности всевозможного вычислительного и телекоммуникационного оборудования разного производства, совместное функционирование которого обеспечивается соответствием требованиям международных стандартов.

Термин «открытые системы» подразумевает также, что если вычислительная система соответствует стандартам, то она будет открыта для взаимосвязи с любой другой системой, которая соответствует тем же

стандартам. Это, в частности, относится и к механизмам криптографической защиты информации или к защите от несанкционированного доступа к информации.

Важная заслуга Интернета состоит в том, что он заставил по-новому взглянуть на такие технологии. Во-первых, Интернет поощряет применение открытых стандартов, доступных для внедрения всем, кто проявит к ним интерес. Во-вторых, он представляет собой крупнейшую в мире и, вероятно, единственную сеть, к которой подключается такое множество разных компьютеров. И, наконец, Интернет становится общепринятым средством представления быстроменяющихся новой продукции и технологий на мировом рынке.

В Интернете уже давно существует ряд комитетов, в основном из организаций-добровольцев, которые осторожно проводят предлагаемые технологии через процесс стандартизации. Эти комитеты, составляющие основную часть Рабочей группы инженеров Интернета IETF (Internet Engineering Task Force), провели стандартизацию нескольких важных протоколов, ускоряя их внедрение в Интернете. Непосредственными результатами усилий IETF являются такие протоколы, как семейство TCP/IP для передачи данных, SMTP (Simple Mail Transport Protocol) и POP (Post Office Protocol) для электронной почты, а также SNMP (Simple Network Management Protocol) для управления сетью.

В Интернете популярны протоколы безопасной передачи данных, а именно SSL, IPSec, SET. Перечисленные протоколы появились в Интернете сравнительно недавно как необходимость защиты ценной информации и сразу стали стандартами де-факто.

Протокол SSL (Secure Socket Layer) является сейчас популярным сетевым протоколом с шифрованием данных для безопасной передачи по сети. Он позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи. Протокол SSL обеспечивает защиту данных между сервисными протоколами (такими, как HTTP, FTP и др.) и транспортными протоколами (TCP/IP) с помощью современной криптографии [1].

Спецификация IPSec входит в стандарт IP v.6 и является дополнительной по отношению к текущей версии протоколов TCP/IP. Она разработана Рабочей группой IP Security IETF. В настоящее время IPSec включает три алгоритмо-независимых базовых спецификаций, представляющих соответствующие RFC-стандарты. Протокол IPSec обеспечивает стандартный способ шифрования трафика на сетевом (третьем) уровне IP и защищает информацию на основе сквозного шифрования независимо от работающего приложения, при этом шифруется каждый пакет данных, проходящий по каналу. Это позволяет организациям создавать в Интернете виртуальные частные сети [1, 11].

Протокол SET (Security Electronics Transaction) - перспективный стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через сеть Интернет. Протокол SET основан на использовании цифровых сертификатов по стандарту X.509.

Протокол выполнения защищенных транзакций SET является стандартом, разработанным компаниями MasterCard и Visa при значительном участии IBM, GlobeSet и других партнеров. Он позволяет покупателям приобретать товары через Интернет, используя защищенный механизм выполнения платежей.

SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей через сеть Интернет с использованием пластиковых карточек. SET обеспечивает кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты, а также целостность и секретность сообщения, шифрование ценных и уязвимых данных. Поэтому SET более правильно можно назвать стандартной технологией или системой протоколов выполнения безопасных платежей через Интернет с использованием пластиковых карт. SET позволяет потребителям и продавцам подтвердить подлинность всех участников сделки, происходящей в сети Интернет, с помощью криптографии, в том числе применяя цифровые сертификаты.

Объем потенциальных продаж в области электронной коммерции ограничивается достижением необходимого уровня безопасности информации, который обеспечивают вместе покупатели, продавцы и финансовые институты, обеспокоенные вопросами безопасности в сети Интернет. Как упоминалось ранее, базовыми задачами защиты информации являются обеспечение ее доступности, конфиденциальности, целостности и юридической значимости. SET, в отличие от других протоколов, позволяет решать указанные задачи защиты информации в целом. SET, в частности, обеспечивает следующие специальные требования защиты операций электронной коммерции:

- секретность данных оплаты и конфиденциальность информации заказа, переданной наряду с данными об оплате;
- сохранение целостности данных платежей. Целостность информации платежей обеспечивается с помощью цифровой подписи;
- специальную криптографию с открытым ключом для проведения аутентификации;
- аутентификацию держателя по кредитной карточке. Она обеспечивается применением цифровой подписи и сертификатов держателя карт;
- аутентификацию продавца и его возможности принимать платежи по пластиковым карточкам с применением цифровой подписи и сертификатов продавца;
- аутентификацию того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым карточкам через связь с процесинговой карточной системой.

Аутентификация банка продавца обеспечивается использованием цифровой подписи и сертификатов банка продавца;

- готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;
- безопасность передачи данных посредством преимущественного использования криптографии.

Основное преимущество SET по сравнению со многими существующими системами обеспечения информационной безопасности заключается в использовании цифровых сертификатов (стандарт X509, версия 3), которые ассоциируют держателя карты, продавца и банк продавца с рядом банковских учреждений платежных систем Visa и Mastercard. Кроме того, SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами и интегрируется с существующими системами.

Инфраструктура управления открытыми ключами PKI ***(Public Key Infrastructure)*** предназначена для защищенного управления криптографическими ключами электронного документооборота, основанного на применении криптографии с открытыми ключами. Эта инфраструктура подразумевает использование цифровых сертификатов, удовлетворяющих рекомендациям международного стандарта X.509, и развернутой сети центров сертификации, обеспечивающих выдачу и сопровождение цифровых сертификатов для всех участников электронного обмена документами (см. главу 4).

12.3. Отечественные стандарты информационной безопасности

Исторически сложилось, что в России проблемы безопасности ИТ изучались и своевременно решались в основном в сфере охраны государственной тайны. Аналогичные задачи коммерческого сектора экономики долгое время не находили соответствующих решений.

Информация, содержащаяся в системах или продуктах ИТ, является критическим ресурсом, позволяющим организациям успешно решать свои задачи. Кроме того, частные лица вправе ожидать, что их персональная информация, будучи размещенной в продуктах или системах ИТ, останется приватной, доступной им по мере необходимости и не сможет быть подвергнута несанкционированной модификации.

При выполнении продуктами или системами ИТ их функций следует осуществлять надлежащий контроль информации, что обеспечило бы ее защиту от опасностей типа нежелательного или неоправданного распространения, изменения или потери. Понятие «безопасность ИТ» охватывает предотвращение и уменьшение этих и аналогичных опасностей.

Проблема защиты информации в коммерческой автоматизированной системе имеет свои особенности, которые необходимо учитывать, поскольку они оказывают серьезное влияние на ИБ. Перечислим основные особенности.

1. *Приоритет экономических факторов* - для коммерческой автоматизированной системы важно снизить либо исключить финансовые потери и обеспечить получение прибыли владельцем и пользователями данного инструментария в условиях реальных рисков.

2. *Открытость проектирования*, предусматривающая создание подсистемы защиты информации из средств, широко доступных на рынке и работающих в открытых системах.

3. Юридическая значимость коммерческой информации, которую можно определить как свойство безопасной информации, позволяющее обеспечить юридическую силу электронным документам или информационным процессам в соответствии с законодательством Российской Федерации.

Российские стандарты, регулирующие информационную безопасность, приведены в табл.12.1.

Таблица 12.1

Российские стандарты, регулирующие ИБ

№ п/п	Стандарт	Наименование
1	ГОСТ Р ИСО/МЭК 15408-1-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России
2	ГОСТ Р ИСО/МЭК 15408-2-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России

3	ГОСТ Р ИСО/МЭК 15408-3-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России
4	ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России
5	ГОСТ Р 50922-96	Защита информации. Основные термины и определения. Госстандарт России
6	ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России
7	ГОСТ Р 51275-99	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России
8	ГОСТ Р ИСО 7498-1-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России
9	ГОСТ Р ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России
10	ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
11	ГОСТ 28147-89	Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
12	ГОСТ Р 34.10-2001	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
13	ГОСТ Р 34.11-94	Информационная технология. Криптографическая защита информации. Функция хэширования

В этой таблице указаны нормативные документы по критериям оценки защищенности средств вычислительной техники и автоматизированных систем и документы, регулирующие информационную безопасность (строки 1 - 10). Здесь же перечислены основные нормативные документы по криптографической защите систем обработки информации и информационных технологий (строки 11 - 13).

Стандарты в структуре информационной безопасности выступают как связующее звено между технической и концептуальной стороной вопроса. Введение в 1999 году Международного стандарта ISO 15408 в области обеспечения информационной безопасности имело большое значение как для разработчиков компьютерных информационных систем, так и для их пользователей. Стандарт ISO 15408 стал своего рода гарантией качества и надежности сертифицированных по нему программных продуктов. Этот стандарт позволил потребителям лучше ориентироваться при выборе программного обеспечения и приобретать продукты, соответствующие их требованиям безопасности, и, как следствие этого, повысил конкурентоспособность IT-компаний, сертифицирующих свою продукцию в соответствии с ISO 15408.

С января 2004 года в России действует ***стандарт «Критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408,*** который является аналогом стандарта ISO 15408. Стандарт ГОСТ Р ИСО/МЭК 15408, называемый еще «Общими критериями» (ОК), является на сегодня самым полным стандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования. «Общие критерии» направлены на защиту информации от несанкционированного раскрытия, модификации, полной или частичной потери и применимы к защитным мерам, реализуемым аппаратными, программно-аппаратными и программными средствами.

«Общие критерии» предназначены служить основой при оценке характеристик безопасности продуктов и систем ИТ. Заложенные в стандарте наборы требований позволяют сравнивать результаты независимых оценок безопасности. На основании этих результатов потребитель может принимать решение о том, достаточно ли безопасны ИТ-продукты или системы для их применения с заданным уровнем риска.

Стандарт ГОСТ Р ИСО/МЭК 15408 состоит из трех частей.

В первой части (ГОСТ Р ИСО/МЭК 15408-1 «Введение и общая модель») устанавливается общий подход к формированию требований безопасности и оценке безопасности, на их основе разрабатываются основные конструкции (профиль защиты и задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки по методологии «Общих критериев» определяются исходя из целей безопасности, которые основываются на анализе назначения объекта оценки и условий среды его использования (угроз, предположений, политики безопасности).

Вторая часть (ГОСТ Р ИСО/МЭК 15408-2 «Функциональные требования безопасности») содержит универсальный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Третья часть (ГОСТ Р ИСО/МЭК 15408-3 «Требования доверия к безопасности») включает в себя систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. Здесь же содержатся оценочные уровни доверия, определяющие шкалу требований, которые позволяют с возрастающей степенью полноты и строгости оценить проектную, тестовую и эксплуатационную документацию, правильность реализации функций безопасности объекта оценки, уязвимости продукта или системы ИТ, стойкость механизмов защиты и сделать заключение об уровне доверия к безопасности объекта оценки.

Обобщая вышесказанное, можно отметить, что каркас безопасности, заложенный частью 1 стандарта ГОСТ Р ИСО/МЭК 15408, заполняется содержимым из классов, семейств и компонентов в части 2, а третья часть определяет, как оценить прочность всего «строения». Стандарт отражает достижения последних лет в области информационной безопасности. Впервые документ такого уровня содержит разделы, адресованные потребителям, производителям и экспертам по оценке безопасности ИТ-продуктов.

Главные достоинства стандарта ГОСТ Р ИСО/МЭК 15408:

- полнота требований к информационной безопасности;
- гибкость в применении;
- открытость для последующего развития с учетом новейших достижений науки и техники.

Вопросы для самоконтроля

1. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
2. Назовите основные международные стандарты информационной безопасности.
3. Дайте краткую характеристику международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000).
4. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности»?
5. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий.
6. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.
7. Назовите стандарты информационной безопасности для Интернета.
8. Каковы назначение и особенности функционирования протокола SET (Security Electronics Transaction)?
9. Каковы назначение и функциональность протоколов SSL (Secure Socket Layer) и IPSec? В чем эти протоколы существенно различаются?
10. Каковы назначение и функциональность инфраструктуры управления открытыми ключами PKI?
11. Перечислите российские стандарты безопасности информационных технологий.
12. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408? Назовите и охарактеризуйте три основные части этого стандарта.

Литература

1. ***Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.*** Защита информации в сети - анализ технологий и синтез решений. - М.: ДМК Пресс, 2004. - 616 с.: ил.

2. ***Дишунян В.Л., Шаньгин В.Ф.*** Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты. - М.: ООО «Издательство АСТ»: Издательство «НТ Пресс», 2004. - 695 с.: ил.

3. ***Зима В.М., Молдовян А.А., Молдовян Н.А.*** Безопасность глобальных сетевых технологий. - СПб.: БХВ-Петербург, 2001. - 320 с.: ил.

4. ***Коннолли Т., Бегг К.*** Базы данных. Проектирование, реализация и сопровождение. Теория и практика. - 3-е изд.: Пер. с англ. - М.: Издательский дом «Вильямс», 2003. - 1440 с.: ил.

5. ***Мамаев М., Петренко С.*** Технологии защиты информации Интернета. Специальный справочник. - СПб.: Питер, 2002. - 848 с.

6. ***Олифер В.Г., Олифер Н.А.*** Новые технологии и оборудование IP-сетей. - СПб.: БХВ - Санкт-Петербург, 2000. - 512 с.

7. ***Панасенко С.П., Батура В.П.*** Основы криптографии для экономистов: учеб. пособие / ***Под ред. Л.Г. Гагариной***. - М.: Финансы и статистика, 2005. - 176 с.: ил.

8. ***Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.*** Защита информации в компьютерных системах и сетях. - 2-е изд. - М.: Радио и связь, 2001. - 376 с.: ил.

9. ***Садердинов А.А., Трайнев В.А., Федулов А.А.*** Информационная безопасность предприятия. - М.: Изд. Дашков и Ко., 2006. - 336 с.: ил.

10. ***Смирнов С.Н.*** Безопасность систем баз данных. - М.: Гелиос АРБ, 2007. - 352 с.: ил.

11. ***Соколов А.В., Шаньгин В.Ф.*** Защита информации в распределенных корпоративных сетях и системах. - М.: ДМК Пресс, 2002. - 656 с.: ил.

12. Теоретические основы компьютерной безопасности: учеб. пособие для вузов / ***П.Н.Девянин, О.О.Михальский, Д.И. Правиков и др.*** - М.: Радио и связь, 2000. - 192 с.

13. ***Чмора А.Л.*** Современная прикладная криптография. - М.: Гелиос АРВ, 2001. - 256 с.

14. ***Шаньгин В.Ф.*** Защита компьютерной информации. Эффективные методы и средства. - М.: ДМК Пресс, 2008. - 544 с.: ил.

15. ***Шарков А.Е., Сердюк В.А.*** Защита корпоративного почтового документооборота // Сети и системы связи. - 2003. - № 13.

Интернет-ресурсы

16. ***Беляев А.В.*** Методы и средства защиты информации // Документ. - URL: http://www.citforum.ru/internet/infsecure/its2000_01.shtml.

17. ***Касперский Е.*** Компьютерные вирусы. Книга - Электронное издание. - URL: http://www.kaspersky.ru/.

18. Обзор Windows Vista / Безопасность. - URL: http://www.webdocs.ru/content-494.html.

19. Решения по построению систем ИБ. УЦСБ. - URL: http://www.ussc.ru/index.php.

20. Решения IBM для обеспечения информационной безопасности. - URL: http://www.ibm.com/ru.

21. Решения CISCO для обеспечения информационной безопасности. - URL: http://www.cisco.com/ru.

22. Решения компании Информзащита. Защищенный доступ к базам данных. - URL: http://www.infosec.ru/sitemap/.

23. Решение ЭЛВИС-ПЛЮС по созданию подсистемы защиты от воздействия вредоносных программ и вирусов. - URL: http://www.elvis.ru/solutions_system.shtml.

24. ***Самодуров А.*** Особенности защиты электронного документооборота. CNews Analytics. - 2006. - URL: http://www.cnews,ru/reviews/free/security 2006/articles/e-docs/.

25. Семейство продуктов CSP VPN. Компания «С-Терра СиЭсПи». - 2008. - URL: http://www.s-terra.com/index.htm.

26. ***Скородумов Б.И.*** Стандарты для безопасности электронной коммерции в сети Интернет. - URL: http://www.stcarb.comcor.ru.

27. Электронный документооборот. - URL: http://www.directum-journal.ru/.

28. Семейство стандартов IEEE 802.11. - URL: http://www.wireless.ru/wireless/wrl_base80211.

29. Система электронного документооборота DIRECTUM. - URL: http://www.directum.ru/314838.shtml.

30. Advanced Encryption Standard (AES) Development Effort. - February 2001. - URL: csrc.nist.gov/CryptoToolkit/aes/index2.html.