Информационная безопасность

1. **Модели безопасности ОС. Дискреционные и мандатные модели доступа.**

**Модель безопасности ОС** – это формальное описание политики безопасности, определяющее правила доступа субъектов к объектам. Модели позволяют математически доказать безопасность системы и проверить корректность ее реализации.

**Дискреционная модель доступа (DAC)** основана на принципе владения ресурсами. Владелец объекта сам определяет права доступа к нему для других субъектов. Права описываются матрицей доступа, где строки соответствуют субъектам, столбцы – объектам, а ячейки содержат разрешенные операции (чтение, запись, выполнение). На практике матрица реализуется через списки контроля доступа (ACL) или списки возможностей.

Основной недостаток DAC – невозможность контроля информационных потоков, что приводит к проблеме “троянского коня”. Модель Харисона-Рузо-Ульмана доказала, что в общем случае невозможно алгоритмически определить, приведет ли произвольная последовательность операций к нежелательной передаче прав.

**Мандатная модель доступа (MAC)** использует централизованно назначаемые метки безопасности для субъектов и объектов. Доступ определяется сравнением этих меток согласно заданной политике. Пользователи не могут изменять метки, что позволяет контролировать информационные потоки на уровне системы.

Модель Белла-Лападулы обеспечивает конфиденциальность через два принципа: - “Нет чтения вверх” (No Read Up) – субъект не может читать объекты с более высоким уровнем секретности - “Нет записи вниз” (No Write Down) – субъект не может записывать в объекты с более низким уровнем секретности

**Ролевая модель (RBAC)** объединяет достоинства дискреционного и мандатного подходов. Права доступа ассоциируются с ролями, а пользователям назначаются роли. Это значительно упрощает администрирование в крупных системах.

**SELinux** – практическая реализация мандатного контроля доступа для Linux. Использует контексты безопасности и политики, определяющие разрешенные взаимодействия между процессами и ресурсами системы.

2. **Критерии безопасности информационных систем. Стандарты безопасности информационных систем.**

**Критерии безопасности** – это фундаментальные принципы, обеспечивающие защиту информационных систем. Основные критерии формируют модель безопасности CIA:

**Конфиденциальность** – информация доступна только авторизованным пользователям. Обеспечивается через разграничение доступа, шифрование и контроль информационных потоков. Нарушение конфиденциальности приводит к утечкам данных.

**Целостность** – защита информации от несанкционированной модификации, подтверждение ее достоверности. Реализуется с помощью цифровых подписей, контрольных сумм и журналирования изменений. Нарушение целостности может привести к подлогу данных.

**Доступность** – авторизованные пользователи могут своевременно получить доступ к информации. Поддерживается через резервное копирование, отказоустойчивые системы и защиту от DoS-атак. Нарушение доступности приводит к отказу в обслуживании.

К расширенным критериям относятся: - **Неотказуемость** – невозможность отрицания совершенных действий - **Подотчетность** – однозначная привязка действий к субъектам

**Стандарты безопасности** предоставляют методологии и требования для оценки и обеспечения защиты систем.

**Международные стандарты:** - **ISO/IEC 27000** определяет принципы построения систем управления информационной безопасностью (СУИБ). ISO 27001 содержит требования к СУИБ, а ISO 27002 – рекомендации по практикам защиты.

**Common Criteria (ISO/IEC 15408)** устанавливает структуру для спецификации требований безопасности и оценки соответствия продуктов. Включает семь уровней доверия (EAL1-EAL7), профили защиты (PP) и задания по безопасности (ST).

**Российские стандарты** включают ГОСТ Р ИСО/МЭК 15408 и руководящие документы ФСТЭК, определяющие требования к защите различных типов информационных систем.

Стандарты эволюционировали от простых моделей (“Оранжевая книга” TCSEC) к комплексным международным подходам (Common Criteria), отражая рост сложности угроз и систем защиты.

**3. Применение межсетевых экранов для защиты корпоративных сетей.**

**Межсетевой экран (МЭ)** – это система, контролирующая и фильтрующая сетевой трафик на границе сетей согласно заданной политике безопасности. Основная задача МЭ – создание контролируемой зоны безопасности между сетями с разным уровнем доверия.

**Типы межсетевых экранов:**

**Пакетные фильтры** работают на сетевом уровне, анализируя IP-адреса, порты и флаги TCP. Они эффективны и быстры, но не могут анализировать содержимое пакетов и контекст соединений. Пример: базовые правила iptables в Linux:

iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
iptables -P INPUT DROP

**Шлюзы сеансового уровня** отслеживают состояние соединений (Stateful Inspection), позволяя создавать более интеллектуальные правила фильтрации. Они могут определять, является ли пакет частью установленного соединения, что повышает безопасность.

**Шлюзы прикладного уровня (прокси)** анализируют трафик на уровне приложений, понимая специфику протоколов. Это позволяет блокировать сложные атаки и фильтровать контент. Недостатком является более высокая нагрузка на ресурсы.

Современные корпоративные МЭ обычно являются гибридными и включают дополнительные функции: - Трансляция сетевых адресов (NAT) для скрытия внутренней структуры сети - Системы обнаружения и предотвращения вторжений (IDS/IPS) - Фильтрация контента и антивирусная проверка - VPN-шлюзы для безопасного удаленного доступа

**Эффективные стратегии применения МЭ:** - Многоуровневая защита (defense-in-depth) - Принцип минимальных привилегий в правилах - Логирование и аудит событий безопасности - Регулярное обновление политик безопасности

Корректно настроенные межсетевые экраны существенно снижают поверхность атаки корпоративной сети, блокируя несанкционированный доступ и выявляя потенциально опасную активность.

**4. Электронные цифровые подписи. Система PGP. Система S/MIME.**

**Электронная цифровая подпись (ЭЦП)** – это криптографический механизм, обеспечивающий целостность данных, аутентификацию отправителя и неотказуемость.

**Принцип работы ЭЦП** основан на асимметричной криптографии: 1. Отправитель вычисляет хеш-сумму документа, обеспечивая его целостность 2. Хеш шифруется закрытым ключом отправителя, формируя подпись 3. Получатель расшифровывает подпись открытым ключом отправителя 4. Полученный хеш сравнивается с хешем документа для проверки

Безопасность ЭЦП зависит от криптографических алгоритмов (RSA, DSA, ECDSA), функций хеширования (SHA-256, SHA-3) и надежности защиты закрытого ключа.

**PGP (Pretty Good Privacy)** – система шифрования и цифровой подписи, широко используемая для защиты электронной почты. Ключевые особенности:

Гибридное шифрование: асимметричное шифрование для обмена сеансовым ключом, симметричное для шифрования содержимого

Web of Trust – децентрализованная модель доверия, где пользователи сами подписывают открытые ключи друг друга

Открытый стандарт OpenPGP (RFC 4880)

Интеграция с почтовыми клиентами через плагины (Enigmail, GPG4Win)

**S/MIME (Secure/Multipurpose Internet Mail Extensions)** – альтернативный стандарт безопасной электронной почты:

Основан на иерархической модели доверия с использованием сертификатов X.509

Встроенная поддержка в большинстве почтовых клиентов

Более строгий процесс проверки личности через центры сертификации (CA)

Совместимость с корпоративной инфраструктурой PKI

Выбор между PGP и S/MIME зависит от потребностей: PGP более гибок и подходит для индивидуального использования, S/MIME лучше интегрируется с корпоративными системами и обеспечивает более формализованную проверку личности.

**5. Инфраструктура открытых ключей. Техники управления ключами. Основные концепции.**

**Инфраструктура открытых ключей (PKI)** – комплекс технологий, процедур и политик для создания, управления и использования сертификатов открытых ключей.

**Основные компоненты PKI:** - **Удостоверяющий центр (CA)** выпускает и подписывает сертификаты, являясь корнем доверия - **Центр регистрации (RA)** проверяет личность заявителей перед выдачей сертификатов - **Хранилище сертификатов** обеспечивает доступ к действующим сертификатам - **Центр валидации (VA)** проверяет действительность сертификатов через CRL или OCSP

**Сертификат X.509** – стандартный формат, содержащий открытый ключ, информацию о владельце, сроке действия, издателе и цифровую подпись CA.

**Жизненный цикл управления ключами:**

**Генерация ключей** должна обеспечивать надлежащую энтропию и безопасность. Используются аппаратные генераторы случайных чисел (HRNG) или защищенные программные PRNG.

**Распределение ключей** – безопасная передача ключей пользователям. Методы включают физическую передачу, защищенные каналы и протоколы распределения ключей (Диффи-Хеллмана).

**Хранение ключей** критично для безопасности. Закрытые ключи защищаются с помощью аппаратных модулей безопасности (HSM), смарт-карт или защищенных хранилищ с шифрованием.

**Отзыв ключей** происходит при компрометации или истечении срока действия. Реализуется через списки отозванных сертификатов (CRL) или онлайн-протокол проверки статуса (OCSP).

**Модели доверия в PKI:** - **Иерархическая** – единый корневой CA с подчиненными CA - **Сетевая (Web of Trust)** – взаимное подтверждение ключей пользователями - **Мостовая** – специальный Bridge-CA связывает разные иерархии PKI

Успешное функционирование PKI зависит от строгого соблюдения политик безопасности, регулярного аудита и использования защищенных технологий на всех этапах жизненного цикла ключей.

**6. Характеристика и механизмы удаленных атак на распределённые вычислительные системы.**

**Удаленные атаки на распределенные системы** – это несанкционированные действия, осуществляемые через сеть без физического доступа к цели. Их опасность обусловлена масштабируемостью, сложностью обнаружения и возможностью каскадного эффекта.

**Основные типы удаленных атак:**

**Атаки отказа в обслуживании (DoS/DDoS)** направлены на нарушение доступности сервисов: - SYN-флуд – отправка большого количества TCP SYN-пакетов без завершения соединения - Амплификационные атаки – использование асимметрии запрос/ответ в протоколах (DNS, NTP) - Распределенные атаки (DDoS) – атака с множества скомпрометированных устройств (ботнетов)

**Атаки на уровне приложений** эксплуатируют уязвимости в ПО: - SQL-инъекции – внедрение вредоносного кода в SQL-запросы - Межсайтовый скриптинг (XSS) – внедрение JavaScript на веб-страницы - Уязвимости десериализации – манипулирование данными при десериализации объектов

**Атаки “человек посередине” (MITM)** перехватывают и изменяют данные: - ARP-спуфинг – перехват трафика в локальной сети через подмену ARP-таблиц - DNS-спуфинг – перенаправление на вредоносные серверы через подмену DNS-ответов - SSL/TLS-атаки – обход защиты зашифрованных соединений

**Защита от удаленных атак** требует комплексного подхода: - Регулярное обновление ПО для устранения уязвимостей - Многоуровневая защита сети (defense-in-depth) - Использование систем обнаружения и предотвращения вторжений (IDS/IPS) - Фильтрация трафика и построение демилитаризованных зон (DMZ)

**Системы обнаружения атак** делятся на: - Сетевые (NIDS) – анализируют сетевой трафик - Хостовые (HIDS) – мониторят события на конкретных устройствах - Сигнатурные – используют базы известных шаблонов атак - Аномальные – выявляют отклонения от нормального поведения

Эффективная защита требует сочетания технических мер, обучения персонала и регулярного тестирования безопасности.

**7. Идентификация и аутентификация, управление доступом.**

**Идентификация и аутентификация** – фундаментальные процессы безопасности, являющиеся первой линией защиты информационных систем.

**Идентификация** – процесс предъявления субъектом своего идентификатора (логин, email). Она отвечает на вопрос “Кто вы?”

**Аутентификация** – проверка подлинности идентификатора, подтверждение личности. Она отвечает на вопрос “Как доказать, что вы – это вы?”

**Типы аутентификации** классифицируются по факторам проверки: - **Знание (что-то знаю)**: пароли, PIN-коды, секретные вопросы - **Владение (что-то имею)**: смарт-карты, токены, OTP-генераторы, мобильные устройства - **Биометрия (что-то есть)**: отпечатки пальцев, распознавание лица, голоса - **Местоположение (где я)**: геолокация, принадлежность к сети

**Многофакторная аутентификация (MFA)** комбинирует несколько факторов, значительно повышая безопасность. Например, пароль (знание) + код из SMS (владение).

**Управление доступом** определяет, какие действия разрешены аутентифицированному пользователю.

**Модели управления доступом:** - **Дискреционная (DAC)**: владельцы ресурсов определяют права доступа (ACL в Windows, права файлов в Unix) - **Мандатная (MAC)**: доступ на основе меток безопасности (SELinux, военные системы) - **Ролевая (RBAC)**: права доступа определяются ролями пользователей - **Атрибутная (ABAC)**: доступ на основе атрибутов субъекта, объекта и среды

**Протоколирование и аудит** дополняют систему защиты, обеспечивая: - Запись действий пользователей для последующего анализа - Обнаружение несанкционированной активности - Восстановление последовательности событий при инцидентах - Сбор доказательств для расследований

**Шифрование** защищает конфиденциальность данных, используя: - Симметричные алгоритмы (AES, ChaCha20) для эффективного шифрования больших объемов данных - Асимметричные алгоритмы (RSA, ECC) для безопасного обмена ключами и цифровых подписей

**Контроль целостности** предотвращает несанкционированные изменения через: - Хеш-функции (SHA-256, SHA-3) - Коды аутентификации сообщений (HMAC) - Цифровые подписи

Эффективная система безопасности требует комплексного применения этих механизмов с учетом принципа многоуровневой защиты.