

Информационная безопасность

Лекция 4.

Программно-аппаратные
средства

Программно-технические меры обеспечения ИБ

- ▶ Под программно-техническими мерами понимается совокупность информационных систем и технологий направленных на обеспечение задач по защите информации.
- ▶ Данные меры позволяют автоматизировать многие задачи по обеспечению информационной безопасности

Программно-технические меры

- ▶ При рассмотрении информационной системы на начальном уровне детализации она может быть рассмотрена как совокупность информационных сервисов, обеспечивающих выполнение основных функциональных задач ИС.
- ▶ К числу сервисов безопасности можно отнести:
 - Идентификация и аутентификация
 - Управление доступом
 - Протоколирование и аудит
 - Шифрование
 - Контроль целостности
 - Экранирование
 - Анализ защищенности
 - Обеспечение отказоустойчивости
 - Обеспечение безопасного восстановления

Программно-технические меры

- ▶ Классификация мер безопасности на основе сервисов безопасности и их места в общей архитектуре ИС:
 - Превентивные
 - Меры обнаружения нарушений
 - Локализирующие зону воздействия
 - Меры по выявлению нарушений
 - Меры восстановления режима безопасности

Особенности современных ИС

- ▶ С точки зрения информационной безопасности наиболее существенными являются следующие аспекты:
 - Корпоративная сеть является распределенной, связи между отдельными частями обеспечиваются внешними провайдерами
 - Корпоративная сеть имеет одно или несколько подключений к Internet
 - Критически важные серверы могут располагаться на различных площадках
 - Для доступа пользователей используются как компьютеры так и другие мобильные устройства
 - В течение одного сеанса работы пользователь обращается к нескольким информационным сервисам
 - Требования доступности информационных сервисов выдвигаются достаточно жесткие
 - Информационная система представляет собой сеть с активными агентами, в процессе работы программные модули передаются с сервера на компьютеры пользователя и т.п.
 - Не все пользовательские системы контролируются администраторами ИС
 - Программное обеспечение и модули полученные по сети не могут рассматриваться как надежные
 - Конфигурация ИС постоянно изменяется на уровнях администрирования данных, программ, аппаратуры

Обеспечение информационной безопасности

- ▶ Обеспечение безопасности информации в КИС подразумевает не просто внедрение каких-то средств защиты, а грамотное и последовательное построение подсистем, входящих в систему обеспечения безопасности информации (СОБИ), причем само построение должно осуществляться в соответствии с результатами анализа актуальных угроз безопасности информации, комплексным подходом при проектировании СОБИ и учитывать необходимость централизованного управления средствами защиты информации.
- ▶ СОБИ должна строиться как иерархическая, многоуровневая система.
- ▶ Комплексный подход, применяемый при построении СОБИ, предусматривает наличие нескольких уровней защиты, которые определяют требования по обеспечению безопасности информации на всех этапах ее обращения в КИС: технологического, пользовательского, сетевого и канального.

Подсистемы системы информационной безопасности

- ▶ **Подсистема поддержки доверенной информационной среды (ДИС)** предназначена для поддержания целостной программно-аппаратной среды КИС, обеспечения гарантий доверительности пользователей КИС к предоставляемой системой информации и сервисам.
- ▶ **Подсистема аутентификации и идентификации** предназначена для проведения процедур аутентификации/идентификации сетевых сущностей, входящих в состав КИС, на всех этапах обработки и обращения информации в КИС. Подсистема тесно взаимодействует подсистемой контроля доступа.

Подсистемы системы информационной безопасности

- ▶ **Подсистема контроля доступа** предназначена для управления и контроля за доступом пользователей к АРМ, серверам, прикладным системам, системным и сетевым сервисам и др., входящим в состав КИС, на базе многоуровневой Политики безопасности.
- ▶ **Подсистема защиты потоков** предназначена для создания доверенных каналов связи между структурными составляющими КИС.
- ▶ **Подсистема аудита и регистрации** осуществляет сбор и хранение информации об общем состоянии программных и технических компонентов, функционирующих отдельно или входящих в состав подсистем безопасности, и предназначена для предварительного анализа данной информации.

Подсистемы системы информационной безопасности

- ▶ **Подсистема управления** - ключевая подсистема СОБИ, предназначенная для оперативного управления как отдельными составляющими СОБИ, так и системой в целом, в соответствии с Политикой безопасности.
- ▶ Подсистема включает в себя такие механизмы, как анализ информации с консолей мониторинга средств защиты, система поддержки принятия решения об оперативном усилении/ослаблении политики безопасности в отдельных элементах или узлах СОБИ и противодействия внешним и внутренним атакам, управление отдельными средствами и комплексами защиты информации и др.

Наборы подсистем защиты

- ▶ СОБИ для каждой организации представляет собой различный набор подсистем (решений), который не является стандартным и различен в зависимости от бизнес-задач, решаемых КИС. Однако можно выделить несколько базовых подсистем, составляющих СОБИ корпоративной информационной системы практически любой организации:
 - Подсистема безопасного подключения корпоративной сети к Интернет
 - Подсистема защиты корпоративной электронной почты
 - Подсистема защиты от вредоносных программ и компьютерных вирусов
 - Подсистема защиты внутренних и внешних информационных потоков
 - Подсистема предотвращения вторжений
 - Подсистема защиты информации персональных компьютеров от НСД
 - Подсистема контроля целостности программной среды
 - Подсистема резервного копирования и восстановления данных

Функциональные подсистемы защиты

IDS - обнаружение вторжений
IPS - предотвращение вторжений
AVP - антивирусная защита
CF - контроль содержимого передаваемых данных
VPN - виртуальные частные сети
ЭЦП - электронная цифровая подпись
МЭ - межсетевой экран



Идентификация и аутентификация

- ▶ Идентификация и аутентификация – основа программно-технических средств ИБ.
- ▶ Идентификация позволяет субъекту указать свое имя в ИС.
- ▶ Аутентификация является мерой подтверждения введенного идентификатора.
- ▶ Аутентификация бывает односторонней (клиент доказывает подлинность серверу) или двусторонней (взаимной).

Парольная аутентификация

- ▶ Использование пароля при идентификации субъекта
- ▶ **Достоинства:** простота и удобства для человека
- ▶ **Недостатки:** обеспечивается слабая защита

Парольная защита

- ▶ Меры по обеспечению надежности парольной защиты:
 - Наложение технических ограничений (длина пароля, алфавит пароля)
 - Управление сроком действия пароля, их периодическая смена
 - Ограничение доступа к файлу паролей
 - Ограничение числа неудачных попыток входа в систему
 - Обучение пользователей
 - Использование программных средств генерации паролей

Одноразовые пароли

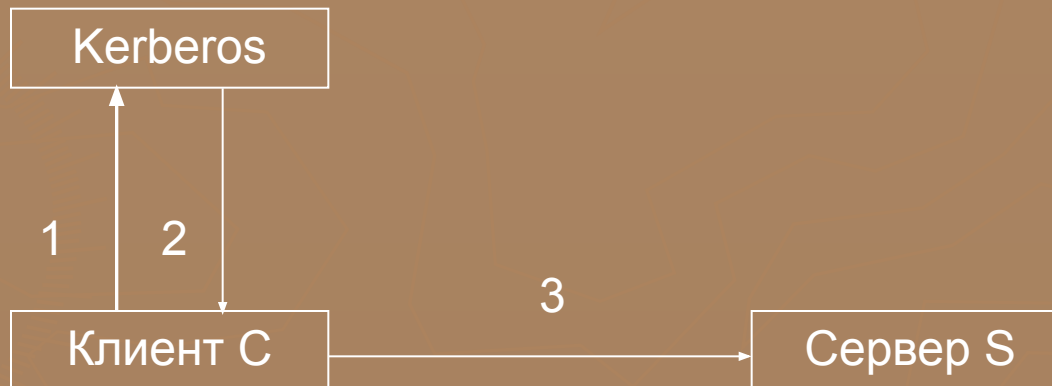
- ▶ Один из подходов повышения надежности парольной схемы – использование одноразовых паролей (например система S/Key):
 - В процессе аутентификации используется односторонняя функция f , данная функция известна пользователю и серверу аутентификации
 - Задан ключ K , известный только пользователю
 - На этапе начального администрирования функция f применяется к ключу K n раз, результат сохраняется на сервер
 - Во время аутентификации сервер присылает на пользовательскую систему число $(n-1)$
 - Пользователь применяет функцию f к секретному числу $(n-1)$ раз и отправляет результат серверу
 - Сервер применяет функцию f к полученному от пользователя значению и сравнивает с ранее сохраненной величиной. В случае совпадения подлинность считается установленной, сервер запоминает присланное значение и уменьшает на единицу счетчик.

Аутентификация Kerberos

- ▶ Схема Kerberos предназначена для решения задачи аутентификации в открытой сети с использованием третьей доверенной стороны.
- ▶ Чтобы получить доступ к серверу S , клиент C посылает Kerberos запрос, содержащий сведения о клиенте и запрашиваемой услуге. В ответ Kerberos возвращает так называемый **билет**, зашифрованный секретным ключом сервера и копию части информации из билета, зашифрованного секретным ключом клиента. Клиент расшифровывает вторую порцию данных и пересылает ее вместе с билетом серверу. Сервер, расшифровав билет, сравнивает с дополнительной информацией, присланной клиентом. Совпадение будет свидетельствовать о том, что клиент смог расшифровать данные присланные ему Kerberos и тем подтверждает знание секретного ключа и свою подлинность.
- ▶ В схеме Kerberos сами секретные ключи не передаются по сети, они используются только в процессе шифрования.

Аутентификация Kerberos

1. Клиент С -> Kerberos: c, s, \dots клиент направляет Kerberos сведения о себе и запрашиваемом сервере
2. Kerberos -> клиент С: $\{d1\}_{K_c}, \{T_{c.s}\}_{K_s}$ Kerberos возвращает билет, зашифрованный ключом сервера и дополнительную информацию, зашифрованную ключом клиента
3. Клиент С -> сервер S: $d2, \{T_{c.s}\}_{K_s}$ клиент направляет на сервер билет и дополнительную информацию



Использование биометрических данных

- ▶ Для выполнения идентификации/аутентификации пользователей часто используются биометрические данные:
 - Отпечатки пальцев
 - Сетчатка и роговица глаза
 - Геометрия руки и лица
 - Голос и распознавание речи
 - Подпись и работа с клавиатурой

Управление доступом

- ▶ Управление доступом позволяет контролировать те действия, которые субъекты имеют право выполнять над информационными объектами.
- ▶ Традиционная постановка задачи состоит в существовании совокупности субъектов S_i и набора объектов O_j .
- ▶ Задача логического управления состоит в том, чтобы для каждой пары (S_i, O_j) определить множество допустимых операций и контролировать выполнения установленного порядка.
- ▶ Отношение «субъекты-объекты» может быть представлено в виде матрицы, в строках которой перечислены субъекты, в столбцах – объекты доступа. Клетки на пересечении строк и столбцов задают условия и права доступа.
- ▶ Поскольку такая матрица часто оказывается разреженной используются **списки прав доступа**, т.е. фактически столбцы данной матрицы.

Управление доступом

- ▶ Контроль прав доступа производится специальными компонентами программной среды – ядром операционной системы, сервисами безопасности, системой управления базами данных, программными модулями промежуточного слоя.
- ▶ При разрешении доступа проводится анализ следующей информации:
 - Идентификатор субъекта – дискреционный (произвольный) доступ
 - Атрибуты субъекта (метка безопасности, группа пользователей) – мандатный (принудительный) доступ

Управление доступом

- ▶ Недостатки дискреционного (произвольного) доступа:
 - управления доступом требует управления многими объектами, что требует разделение функций управления между многими пользователями
 - права доступа существуют отдельно от данных (позволяет злоумышленнику имеющему доступ к информации записать в доступный всем файл или подменить информацию).

Управление доступом

► Ролевое управление

- Между пользователями и их правами доступа устанавливается промежуточная сущность – роль пользователя в ИС.
- Для каждого пользователя может быть активными несколько ролей, каждая из которых дает определенные права пользователю
- Роль нейтральна по отношению к конкретным видам прав и способам их проверки, реализует объектно-ориентированный подход к управлению пользователями

Управление доступом

- ▶ Рольевое управление определяется понятиями:
 - Пользователь
 - Сеанс работы пользователя
 - Роль (определяемая организационной структурой)
 - Объект (сущность, доступ к которой разграничивается)
 - Операция (выполняемая над объектом)
 - Право доступа

Протоколирование и аудит

- ▶ **Протоколирование** – сбор и накопление информации о событиях ИС (внешних, внутренних, клиентских)
- ▶ **Аудит** – анализ накопленной информации, проводимый оперативно или периодически.

Протоколирование и аудит

- ▶ Позволяет решить следующие задачи:
 - Обеспечение подотчетности пользователей и администраторов ИС
 - Обеспечение реконструкции последовательности событий
 - Обнаружение попыток нарушений ИБ
 - Предоставление информации для выявления и анализа проблем

Протоколирование и аудит

- ▶ События, рекомендуемые для протоколирования в «Оранжевой книге»:
 - Вход в систему
 - Выход из системы
 - Обращение к удаленной системе
 - Операции с файлами
 - Смена привилегий или иных атрибутов безопасности

Протоколирование и аудит

- ▶ При протоколировании рекомендуют записывать следующую информацию:
 - Дата и время события
 - Уникальный идентификатор субъекта – инициатора события
 - Результат события
 - Источник запроса
 - Имена объектов
 - Описание изменений, внесенных в базу данных защиты

Активный аудит

- ▶ Задача активного аудита – выявление подозрительной активности и управление средствами автоматического реагирования на нее
- ▶ Активность противоречащую политике безопасности разделяют:
 - Атаки, направленные на незаконное получение полномочий
 - Действия, выполняемые в рамках полномочий, но нарушающие политику безопасности (злоупотребление полномочиями)

Активный аудит

- ▶ Разделяют ошибки активного аудита первого и второго рода:
 - Ошибки первого рода – пропуск атак
 - Ошибки второго рода – ложные срабатывания
- ▶ Методы активного аудита:
 - Сигнатурный – на основе определения сигнатуры атаки (совокупность условий при которых считается, что атака имеет место) – велики ошибки первого рода (неумение обнаруживать неизвестные атаки)
 - Статистический – на основе анализа выполняемых действий субъектов – велики ошибки второго рода

Шифрование

- ▶ Шифрование – использование криптографических сервисов безопасности. Процедура шифрования – преобразование открытого текста сообщения в закрытый.
- ▶ Современные средства шифрования используют известные алгоритмы шифрования. Для обеспечения конфиденциальности преобразованного сообщения используются специальные параметры преобразования – ключи.

Шифрование

- ▶ Криптографические преобразования используются при реализации следующих сервисов безопасности:
 - Собственно шифрование
 - Контроль целостности
 - Аутентификация

Способы шифрования

- ▶ Различают два основных способа шифрования:
 - Симметричное шифрование (с закрытым ключом)
 - Ассиметричное шифрование (с открытым ключом)

Симметричное шифрование

- ▶ В процессе шифрования и дешифрования используется один и тот же параметр – секретный ключ, известный обеим сторонам
- ▶ Примеры симметричного шифрования:
 - ГОСТ 28147-89
 - DES
 - Blow Fish
 - IDEA
- ▶ Достоинство симметричного шифрования
 - Скорость выполнения преобразований
- ▶ Недостаток симметричного шифрования
 - Известен получателю и отправителю, что создает проблемы при распространении ключей и доказательстве подлинности сообщения

Ассиметричное шифрование

- ▶ В криптографических преобразованиях используется два ключа. Один из них не секретный (открытый) ключ используется для шифрования. Второй, секретный ключ для расшифровывания.
- ▶ Примеры несимметричного шифрования:
 - RSA
 - Алгоритм Эль-Гамала
- ▶ Недостаток асимметричного шифрования
 - низкое быстродействие алгоритмов (из-за длины ключа и сложности преобразований)
- ▶ Достоинства:
 - Применение асимметричных алгоритмов для решения задачи проверки подлинности сообщений, целостности и т.п.

Проверка подлинности

- ▶ Криптографические методы позволяют контролировать целостность сообщений, определять подлинность источников данных, гарантировать невозможность отказа от совершенных действий
- ▶ В основе криптографического контроля целостности лежат два понятия:
 - Хэш-функция
 - Электронная цифровая подпись

Проверка подлинности

- ▶ **Хэш-функция** – трудно обратимое преобразование данных, реализуемое посредством симметричного шифрования со связыванием блоков. Результат шифрования последнего блока и служит результатом хэширования.
- ▶ Для проверки целостности данных сравнивается хэш-функция контролируемых данных и ранее вычисленный результат ее применения (дайджест)

Контроль целостности

- ▶ Электронная цифровая подпись выполняет роль обычной подписи в электронных документах для подтверждения подлинности сообщений – данные присоединяются к передаваемому сообщению, подтверждая подлинность отправителя сообщения
- ▶ При формировании цифровой подписи по классической схеме отправитель:
 - Применяет к исходному тексту хэш-функцию
 - Дополняет хэш-образ до длины, требуемой в алгоритме создания ЭЦП
 - Вычисляет ЭЦП по хэш-образу с использованием секретного ключа создания подписи
- ▶ Получатель, получив подписанное сообщение, отделяет цифровую подпись от основного текста и выполняет проверку:
 - Применяет к тексту полученного сообщения хэш-функцию
 - Дополняет хэш-образ до требуемой длины
 - Проверяет соответствие хэш-образа сообщения полученной цифровой подписи с использованием открытого ключа проверки подписи