ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №9
ПОСТРОЕНИЕ ЗАЩИЩЕННЫХ КС

Подготовил: Ковалев М.А.

Цель презентации:

- Рассмотреть построение защищенных КС

Задачи:

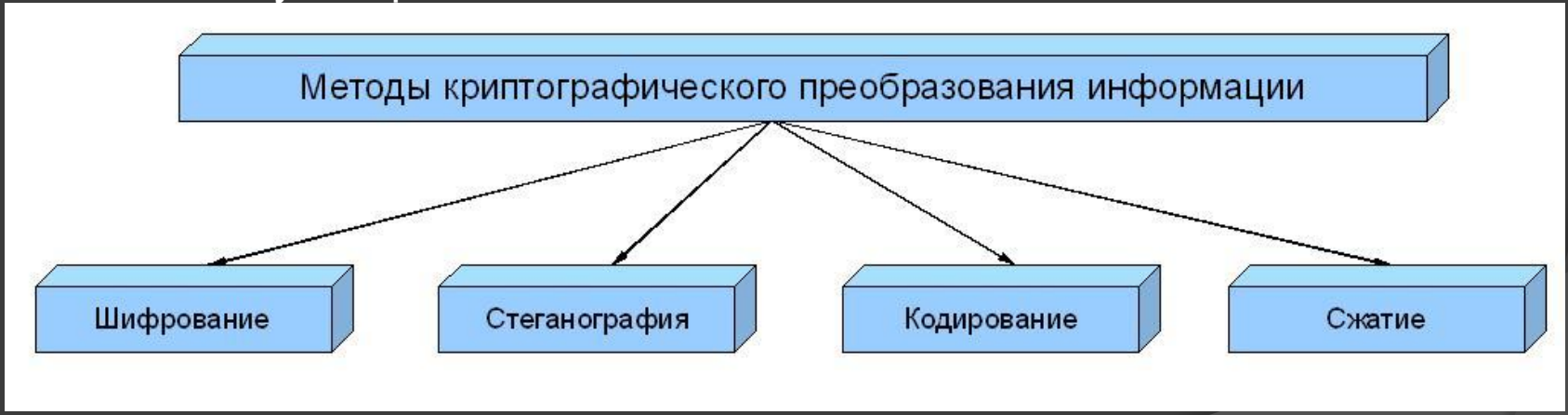
- Указать Основные методы защиты памяти
- Разобрать Построение защищенных КС

Построение защищенных КС

Криптография (от древне-греч. κρυπτος – скрытый и γραφω – пишу) – наука о методах обеспечения конфиденциальности и аутентичности информации.

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

- защиту конфиденциальности;



Основные методы защиты памяти

Защита памяти (англ. Memory protection) — это способ управления правами доступа к отдельным регионам памяти. Используется большинством многозадачных операционных систем. Основной целью защиты памяти является запрет доступа процессу к той памяти, которая не выделена для этого процесса. Такие запреты повышают надежность работы как программ так и операционных систем, так как ошибка в одной программе не может повлиять непосредственно на память других приложений. Следует различать общий принцип защиты памяти и технологии ASLR или NX-бит.

Методы :

- Сегментирование памяти
- Страничная память
- Механизм ключей защиты
- Симуляция сегментации
- Адресация основанная на Capability

Цифровая подпись

Электро́нная по́дпись (ЭП), Электро́нная цифровая по́дпись (ЭЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Защита от сбоев программно-аппаратной среды

- **Защита от сбоев в электропитании**
- **Защита от сбоев процессоров**
- **Защита от сбоев устройств для хранения информации**
- **Защита от утечек информации электромагнитных излучений**

Аддитивная модель

При использовании аддитивной модели, определение ценности базируется на экспертных оценках компонент данной информации, и при объективности денежных оценок её компонент, подсчитывается искомая величина — их сумма в денежном эквиваленте. Основная проблема заключается в том, что количественная оценка компонент информации часто оценивается необъективно, даже при её оценке высококвалифицированными специалистами — причина заключается в неоднородности компонент информации в целом. Для решения этой проблемы принято использовать иерархическую относительную шкалу, которая представляет собой линейный порядок, с помощью которого сравниваются отдельные компоненты защищаемой информации по ценности одна относительно другой.

Порядковая шкала

Существуют случаи, когда не имеется необходимости или возможности установки соответствия ценности информации в денежных единицах (например, информация личного характера, военная или политическая информация, оценка которой в денежном эквиваленте может быть неразумной), но при этом может иметь смысл сравнительная оценка отдельных информационных компонент одной компоненты относительно другой. В качестве примера можно рассмотреть ситуацию в государственных структурах, где информация разбивается по грифам секретности.

Основные уровни защиты информации

- Программно-технический уровень.
- Процедурный уровень.
- Административный уровень.
- Законодательный уровень.

Выводы:

- Указали основные методы защиты памяти
- Разобрали построение защищенных КС