

Тема 7

Методы защиты информации в
компьютерных сетях

Содержание темы

- Модели информационной безопасности.
- Организационные методы.
- Аппаратные методы.
- Программные методы.
- Модели информационной безопасности.
- Триада «Конфиденциальность, доступность, целостность».
- Гексада Паркера.
- Модель STRIDE.

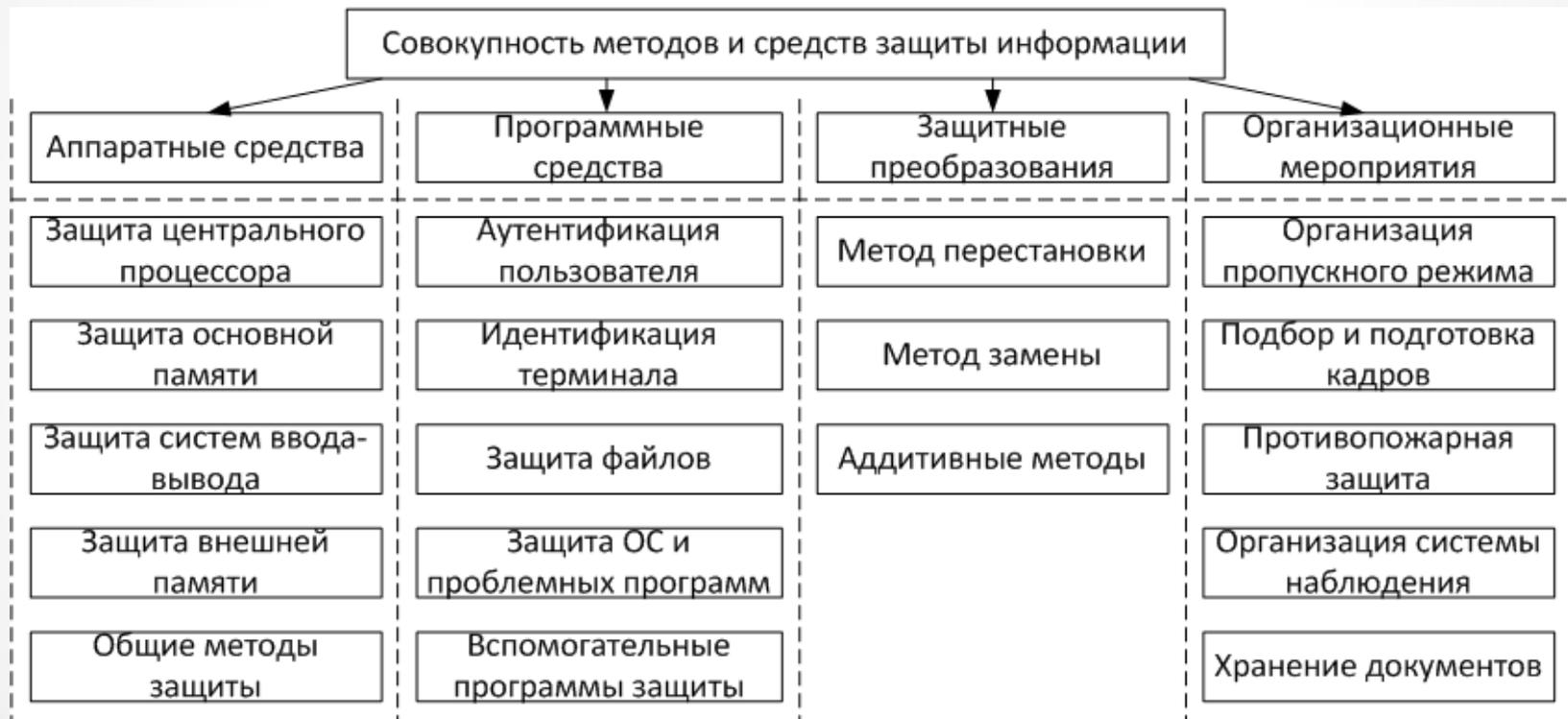
Классификация методов защиты информации

Методы и средства защиты информации являются технической основой системы защиты информации.

Совокупность защитных методов и средств включает в себя:

- программные методы;
- аппаратные средства;
- защитные преобразования;
- организационные мероприятия.

Классификация методов защиты информации



Аппаратные методы ЗИ

Сущность **аппаратной** или **схемной защиты** состоит в том, что в устройствах и технических средствах обработки информации предусматривается наличие специальных технических решений, обеспечивающих защиту и контроль информации.

К аппаратным методам защиты информации относятся:

- электронный замок;
- электро-магнитный экран и т. п.

Программные методы ЗИ

Программные методы защиты – это совокупность алгоритмов и программ, обеспечивающих разграничение доступа и исключение несанкционированного использования информации.

К программным методам защиты информации относятся:

- антивирусная программа;
- программный брандмауэр и т. п.

Методы защитных преобразований

Сущность **методов защитных преобразований** состоит в том, что информация, хранимая в системе и передаваемая по каналам связи, представляется в некотором коде, исключающем возможность ее непосредственного использования.

К методам защитных преобразований относятся:

- методы замены;
- методы перестановки и т. п.

Организационные мероприятия по ЗИ

Организационные мероприятия по защите включают в себя совокупность действий по подбору и проверке персонала, строгое регламентирование процесса разработки и функционирования информационной системы.

К организационным мероприятиям по защите информации относятся:

- организация пропускного режима в здание;
- система видеонаблюдения и т. п.

Классификация методов защиты информации



Модели информационной безопасности

Информационная безопасность - это процесс обеспечения конфиденциальности, доступности, целостности и информации.

Триада «**конфиденциальность, доступность, целостность**» только одна из существующих моделей информационной безопасности.

Эта популярная до сих пор модель была предложена Джери Зальцером и Майком Шредером в 1975 году.

Модели информационной безопасности



Модели информационной безопасности

Гексада Паркера – одна из наиболее известных альтернатив триаде КДЦ. Она появилась в 1998 году.

Аутентичность – это состояние системы, при котором пользователь не может выдать себя за другого, а документ всегда имеет достоверную информацию об его источнике.

Владение – это состояние системы, при котором физический контроль над устройством или другой средой хранения информации предоставляется только тем, кто имеет на это право.

Полезность – это такое состояние информационной системы, при котором обеспечивается удобство практического использования информации и связанных с ней процедур.

Модели информационной безопасности



Модели информационной безопасности

Модель STRIDE – альтернатива триаде КДЦ и гексаде Паркера. Она используется компанией Microsoft для разработки безопасного программного обеспечения.

В соответствии с этой моделью информационная система находится в безопасности, если она защищена от следующих видов нарушений информационной безопасности:

S poofing	Подмена данных
T ampering	Изменение данных
R epudiation	Отказ в ответственности
I nformation Disclosure	Разглашение сведений
D enial of Service	Отказ в обслуживании
E levation of Privilege	Захват привилегий