Тема 4

Методы защиты информации

Содержание темы

- Классификация методов защиты информации по характеру проводимых мероприятий.
- Аппаратные методы.
- Программные методы.
- Организационные методы.
- Модели информационной безопасности.
- Обеспечение конфиденциальности, доступности и целостности информации.

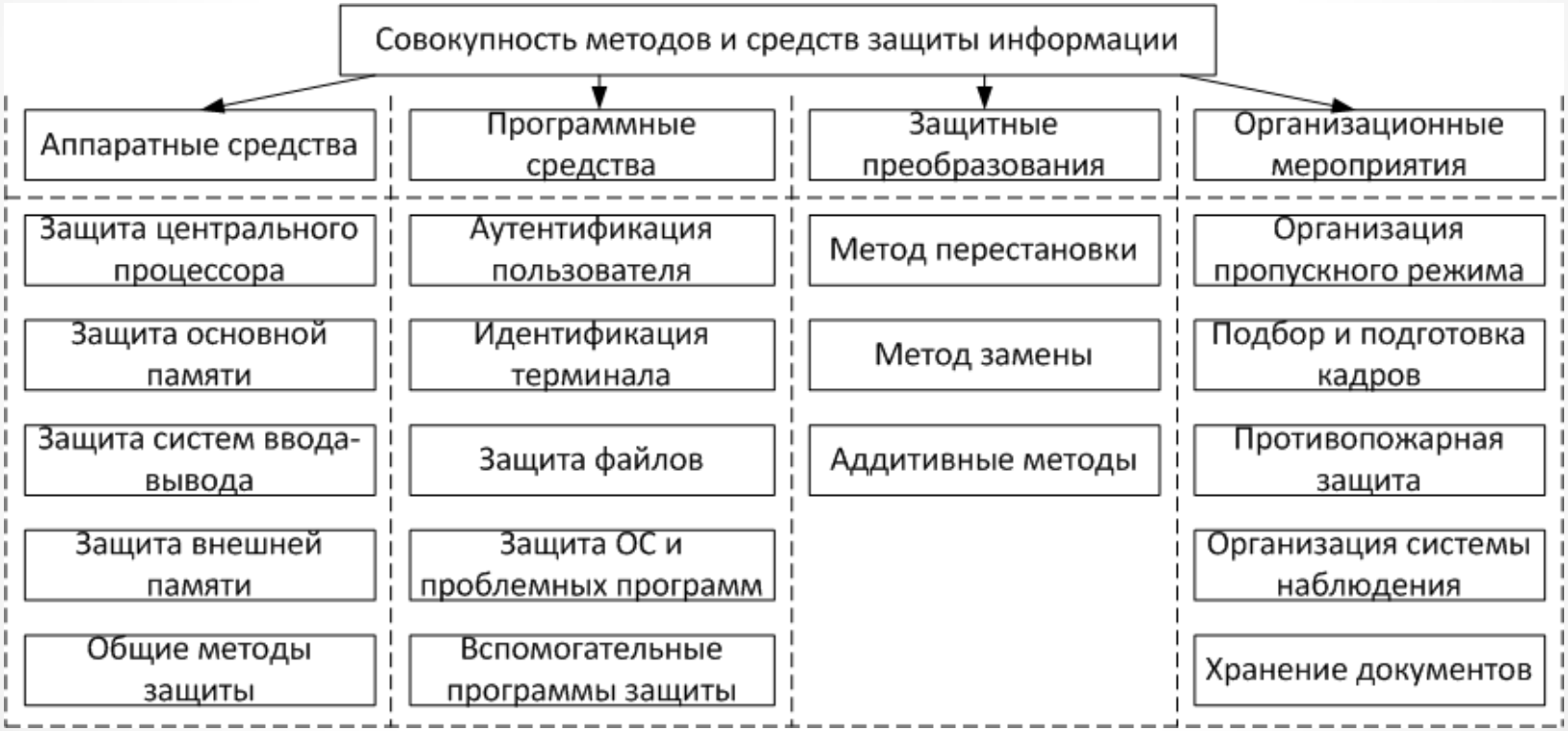
Классификация методов защиты информации

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:

Spuffing	Подмена данных
Tampering	Изменение данных
Repudiation	Отказ в ответственности
Information Disclosure	Разглашение сведений
Denial of Service	Отказ в обслуживании
Elevation of Privilege	Захват привилегий

Обеспечение конфиденциальности

Служба конфиденциальности обеспечивает секретность информации. Правильно сконфигурированная, эта служба открывает доступ к информации только аутентифицированным пользователям.

Служба конфиденциальности должна учитывать различные способы представления информации – в виде распечаток, файлов или пакетов, передающихся по сетям.

Механизмы обеспечения конфиденциальности	Контроль физической безопасности
	Контроль доступа к файлам на компьютере
	Шифрование файлов
Требования к конфиденциальности файлов	Идентификация и аутентификация
	Правильная настройка компьютерной системы
	Правильное управление ключами при использовании шифрования

Обеспечение доступности

Служба обеспечения доступности информации поддерживает ее готовность к работе, позволяет обращаться к компьютерным системам, хранящимся в этих системах данным и приложениям.

Для сохранения важной информации самым простым способом является создание ее резервных копий и размещение их в безопасном месте.

Обеспечение целостности

Служба обеспечения целостности следит за правильностью информации.

При должном уровне организации эта служба дает пользователям уверенность в том, что информация является верной, и ее не изменил никто из посторонних.

Способы защиты бумажных документов от подделки: подпись на каждой странице, подшивка документов в папки, изготовление нескольких копий документа.

Основным способом защиты целостности электронных документов или файлов является контроль над доступом к ним на компьютере.