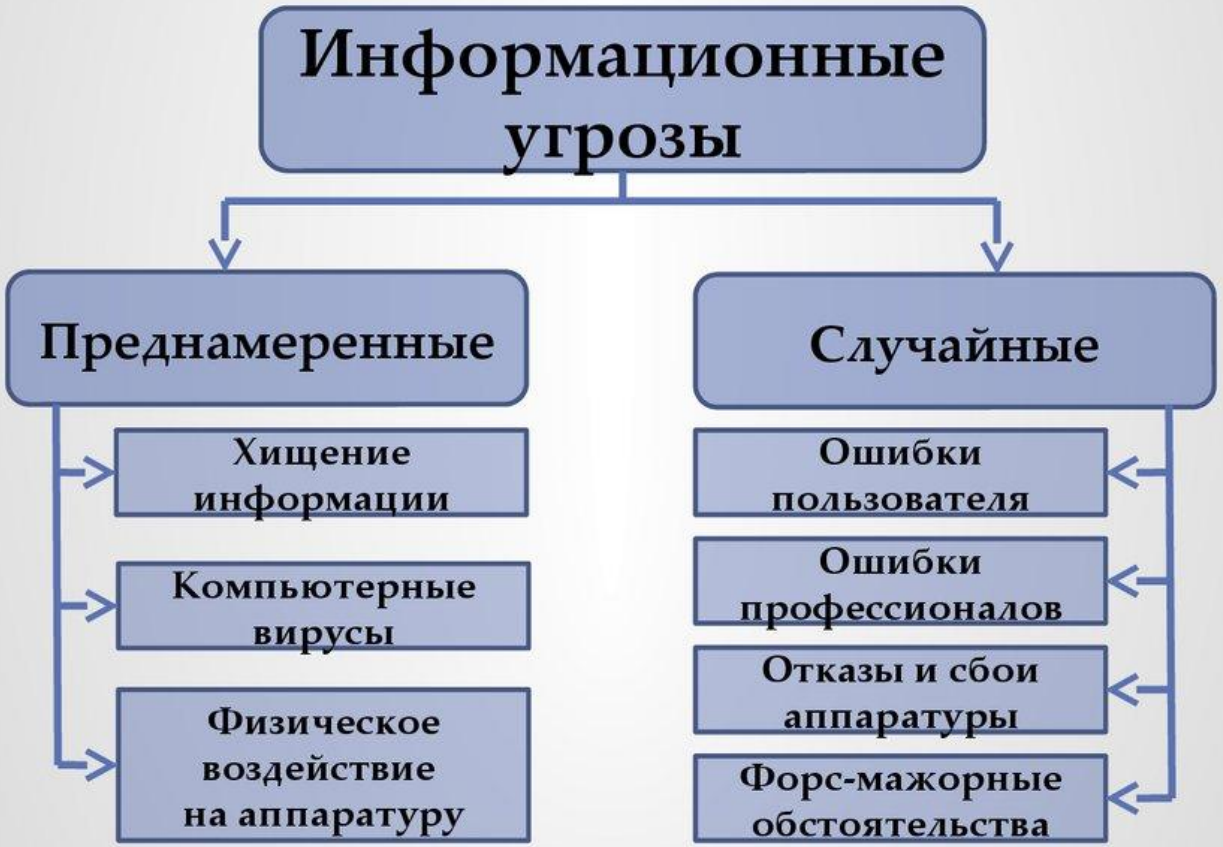
Защита информации

Защита информации- это комплекс мероприятий , направленных на обеспечение информационной безопасности

Защищаемая информация-информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или собственников информации

Виды информационных угроз



Существуют следующие виды защиты

Виды и методы защиты информации

Вид защиты	Метод защиты
От сбоев оборудования	• Архивирование файлов (со сжатием или без); • резервирование файлов
От случайной потери или искажения информации, хранящейся в компьютере	• Запрос на подтверждение выполнения команд, изменяющих файлы; • установка специальных атрибутов документов и программ; • возможность отмены неверного действия или восстановления ошибочно удалённого файла; • разграничение доступа пользователей к ресурсам файловой системы

Разберем более подробно методы защиты

Методы защиты

1. ***Управление доступом*** - метод защиты информации регулированием использования всех ресурсов системы, включающий следующие функции:
   - идентификация ресурсов системы;
   - установление подлинности (аутентификация) объектов или субъектов системы по идентификатору;
   - проверка полномочий в соответствии с установленным регламентом;
   - разрешение и создание условий работы в соответствии с регламентом;
   - регистрация обращений к защищаемым ресурсам;
   - реагирование при попытках несанкционированных действий.
1. ***Препятствие*** - метод физического преграждения пути нарушителю к защищаемым ресурсам системы.
2. ***Маскировка*** - метод защиты информации путем ее криптографического закрытия.
3. ***Регламентация*** - метод защиты информации, создающей такие условия автоматизированной обработки, хранения и передачи информации, при которых возможности несанкционированного доступа к ней минимизируются.
4. ***Принуждение*** - метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать регламент под угрозой ответственности.
5. ***Побуждение*** - метод защиты информации, который мотивирует пользователей и персонал системы соблюдать сложившиеся морально-этические нормы.

Несанкционированный доступ

- - действия, нарушающие установленный порядок доступа или правила разграничения, доступ к программам и данным, который получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или работу с этими ресурсами . Для предотвращения несанкционированного доступа осуществляется контроль доступа.

Вредоносная программа (буквальный перевод англоязычного термина **Malware**, **mal***icious* — злонамеренный и *soft***ware** — программное обеспечение) — злонамеренная программа, то есть программа, созданная со злым умыслом или злыми намерениями.

К ним относятся:

- **Вирусы, черви, троянские и хакерские программы**

Потенциально опасное программное обеспечение

Шпионское, рекламное программное обеспечение

Криптография

- *наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства.*
- *В криптографии используются различные шифры.*
- *Одним из первых считается шифр Цезаря.*
- *Шифры криптографии использовались во время гражданской войны в США, Второй мировой*

- Методы криптографии позволяют осуществлять не только засекречивание сообщений. Существуют приемы защиты целостности сообщения, позволяющие обнаружить факты изменения или подмены текста, а также подлинности источника сообщения.
- Сравнительно недавно появились технологии *цифровой подписи* и *цифрового сертификата*.

Цифровая подпись

- *Это индивидуальный секретный шифр, ключ которого известен только владельцу . Наличие цифровой подписи говорит о том, что ее владелец подтвердил подлинность содержимого переданного сообщения.*
- *Алгоритм шифрования: закрытый ключ применяется для шифрования, а открытый- для дешифрования.*

Цифровой сертификат

- *сообщение, подписанное полномочным органом сертификации , который подтверждает, что открытый ключ действительно относится к владельцу подписи и может быть использован для дешифрования*