Защита информации

Выполнил: Зырянов Александр
10 а

Меры защиты информации

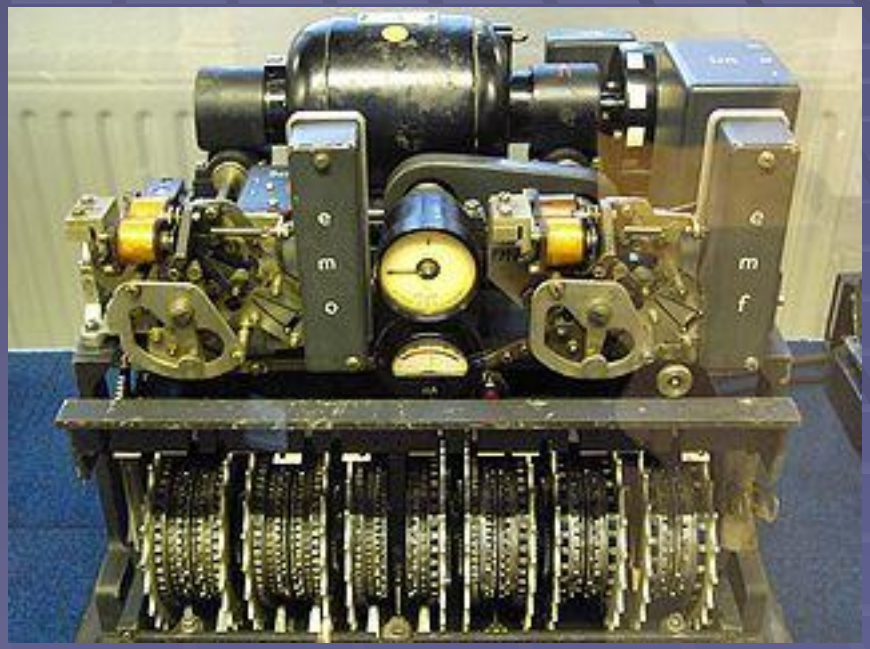
- Организационные меры защиты информации:
- ограничение доступа к помещениям, где информация содержится и обрабатывается;
- допуск только проверенных лиц к конфиденциальной информации;
- хранение информации в закрытых для посторонних сейфах;
- блокировка просмотра содержания обрабатываемых материалов;
- криптографическая защита при передаче каналами связи;
- своевременное уничтожение остаточной информации.
- Организационно-технические меры защиты информации:
- организация независимого питания оборудования, содержащего и обрабатывающего ценную информацию;
- установка кодовых замков;
- использование жидкокристаллических или плазменных дисплеев, струйных принтеров и термопринтеров, избегая высокочастотного электромагнитного излучения;
- уничтожение информации при списании или отправки компьютера в ремонт;
- минимальная защита снятия информации акустическим способом с помощью мягких прокладок, установленных под оборудованием;
- экранирования помещений обработки данных.

Угрозы информационной безопасности

- Угрозы информационной безопасности могут быть классифицированы по различным признакам:
- По аспекту информационной безопасности, на который направлены угрозы:
  - *Угрозы конфиденциальности* (неправомерный доступ к информации).
  - *Угрозы целостности* (неправомерное изменение данных).
  - *Угрозы доступности* (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).
- По степени преднамеренности действий:
  - *Случайные* (неумышленные действия, например, сбои в работе систем, стихийные бедствия).
  - *Преднамеренные* (умышленные действия, например, шпионаж и диверсии).
- По расположению источника угроз:
  - *Внутренние* (источники угроз располагаются внутри системы).
  - *Внешние* (источники угроз находятся вне системы).
- По размерам наносимого ущерба:
  - *Общие* (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба).
  - *Локальные* (причинение вреда отдельным частям объекта безопасности).
  - *Частные* (причинение вреда отдельным свойствам элементов объекта безопасности).
- По степени воздействия на информационную систему:
  - *Пассивные* (структура и содержание системы не изменяются).
  - *Активные* (структура и содержание системы подвергается изменениям).

Криптогра́фия

- **Криптогра́фия** (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — наука о методах обеспечения конфиденциальности(невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.
- Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.



Немецкая криптомашина Lorenz использовалась во время Второй мировой войны для шифрования самых секретных сообщений

Информационная безопасность

- **Информационная безопасность государства** — состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.
- В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Цифровые подписи и сертификаты

- **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).
- **Цифровой сертификат** — выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов.

Источники

- Википедия