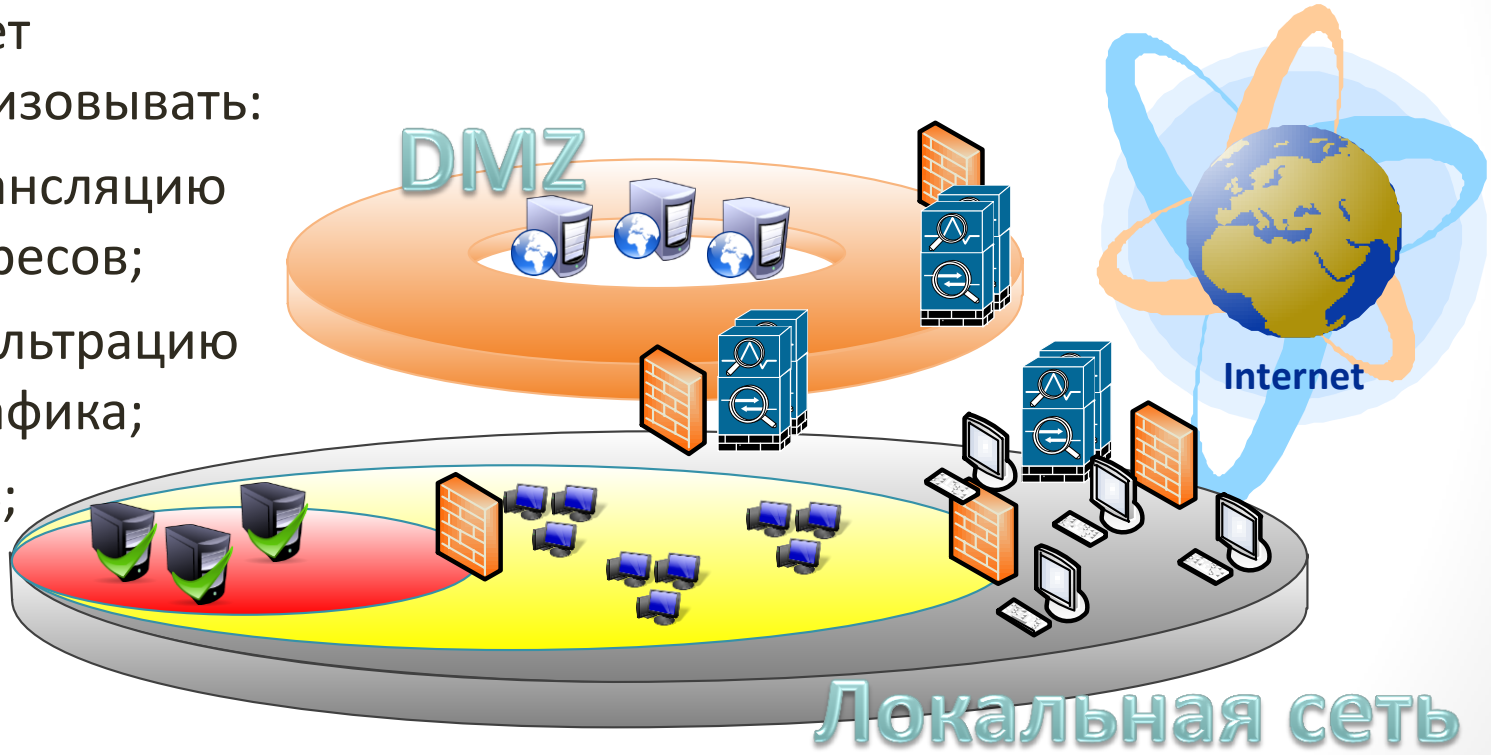
Типовая структура

- Активное сетевое оборудование на границе зон может реализовывать:
  - Трансляцию адресов;
  - Фильтрацию трафика;
  - IDS;



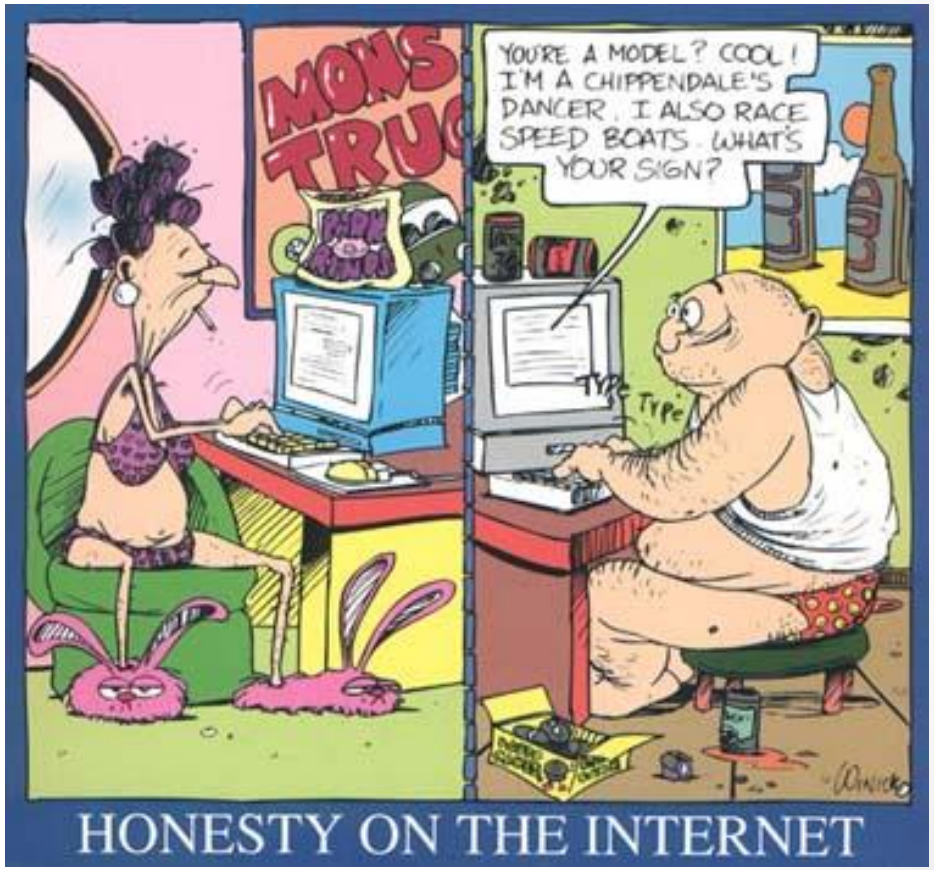
Элементы системы защиты информации

- Защита от НСД:
  - Авторизация;
  - Разграничение доступа.
- Антивирусная защита.
- Надежное хранилище
  - Контроль целостности
  - обеспечение конфиденциальности
- Подсистема управление траффиком.
- Подсистема резервного копирования
- Системы обнаружения (предотвращения) вторжений.
- Система анализа защищенности.
- Криптографическая подсистема.
- Подсистема регистрации событий.

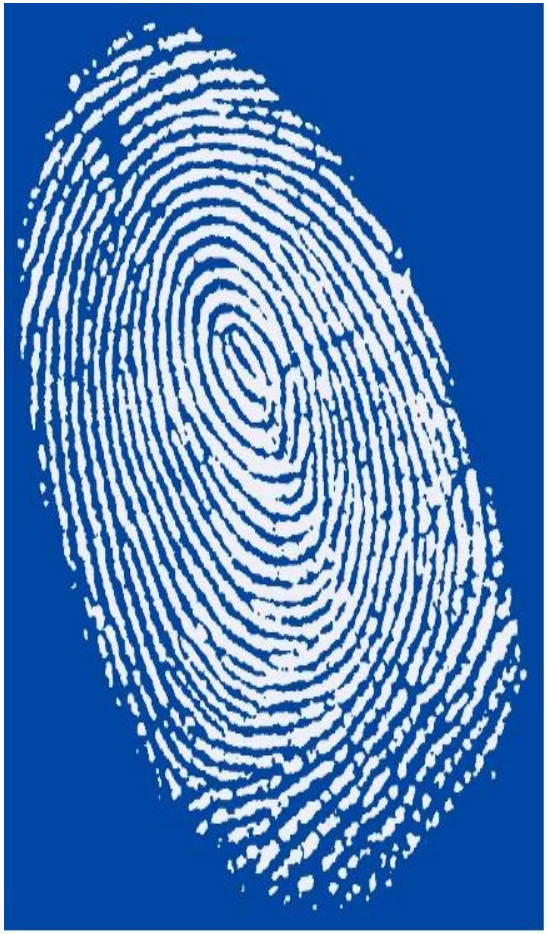
АВТОРИЗАЦИЯ

Идентификация и аутентификация

В целях обеспечения возможности разграничения доступа к ресурсам АС и возможности регистрации событий такого доступа каждый субъект и объект защищаемой АС должен быть однозначно идентифицируем. Для этого в системе должны храниться специальные признаки каждого субъекта и объекта, по которым их можно было бы однозначно опознать.



Аутентификация



- путем проверки знания того, чего не знают другие (паролей, PIN-кодов,ключевых слов);
- путем проверки владения тем, что относительно сложно подделать(карточками, ключевыми вставками и т.п.);
- путем проверки уникальных физических характеристик и параметров (отпечатков пальцев, особенностей радужной оболочки глаз, формы кисти рук и т.п.) самих пользователей при помощи специальных биометрических устройств;
- путем проверки рекомендации (сертификата, специального билета) от доверенного посредника.

Требования к системе

Пользовательские

- Простота пользования
- Минимальные требования по оборудованию
- Возможность быстрого восстановления доступа

Системные

- Безопасное хранение идентифицирующей сущности
- Быстрый доступ к хранилищу
- Гарантия безопасности в случае кражи базы

Хранение паролей

- Хэширование
  - MD5 не обеспечивает надежного хранения
  - В целом менее стоек, чем шифрование
  - Нет проблем с хранением ключей
- Шифрование
  - При достаточной дине ключа обеспечивает надежное хранение
  - Относительно сложен в реализации
  - Проблема с ключами

Банковская идентификация

- Использование генератора кодов
- Независимость от программно-аппаратного обеспечения пользователя
- Верификация подписанных данных

Угрозы

- Фишинг
- Социальная инженерия
- Человеческий фактор

ЦЕЛОСТНОСТЬ

Регистрация событий безопасности

- дата и время события;
- идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
- действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

Оперативное оповещение о событиях безопасности

- подача сигнала тревоги;
- извещение администратора безопасности;
- извещение владельца информации о НСД к его данным;
- снятие программы (задания) с дальнейшего выполнения;
- отключение (блокирование работы) терминала или компьютера, с которого были осуществлены попытки НСД к информации;
- исключение нарушителя из списка зарегистрированных пользователей и т.п.

Контроль целостности программных и информационных ресурсов

Механизм контроля целостности ресурсов системы предназначен для своевременного обнаружения модификации ресурсов системы. Он позволяет обеспечить правильность функционирования системы защиты и целостность обрабатываемой информации

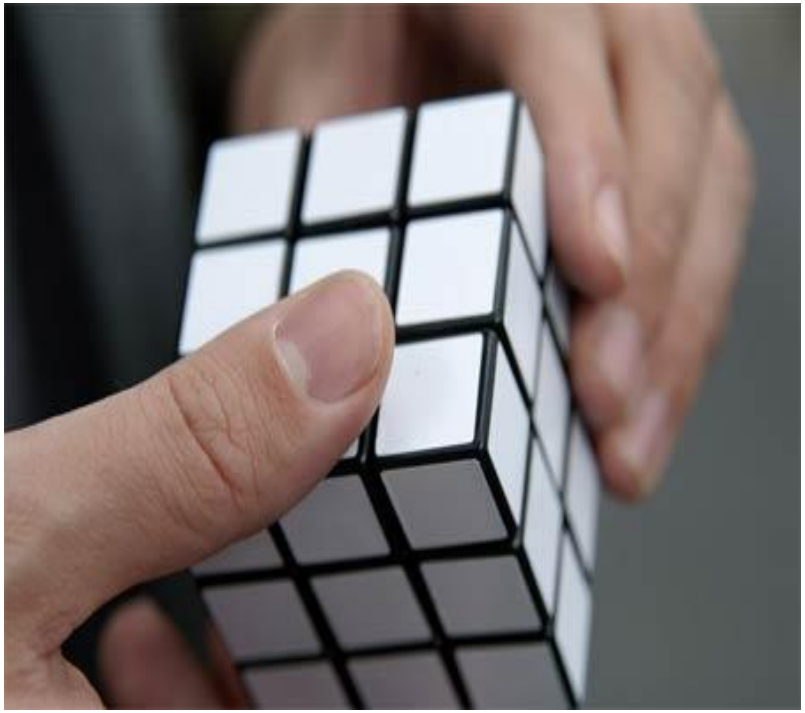
Средства обеспечения целостности

- средствами разграничения доступа, запрещающими модификацию или удаление защищаемого ресурса;
- средствами сравнения критичных ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);
- средствами подсчета контрольных сумм (сигнатур, имитовставок и т.п.);
- средствами электронной цифровой подписи.

Контролируемые ресурсы и параметры

- Ресурсы:
  - файлы и каталоги;
  - элементы реестра;
  - сектора дисков.
- Параметры:
  - содержимое ресурса;
  - списки управления доступом;
  - атрибуты файлов;

Алгоритмы и время контроля



- Алгоритмы:
  - сравнение с эталоном;
  - вычисление контрольных сумм (сигнатур);
  - формирование ЭЦП и имитовставок;
- Время:
  - до загрузки ОС;
  - при наступлении событий;
  - по расписанию.