ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИБЛИОТЕКИ ДОНГТУ

Фомин А.И.
ИВЦ ДонГТУ
г. Алчевск

Потенциальные угрозы потери данных

- Сбои оборудования:
- *сбои кабельной системы;*
- *перебои электропитания;*
- *сбои дисковых систем;*
- *сбои работы серверов, рабочих станций, сетевых карт и т.д.*
- Потери информации из-за некорректной работы программного обеспечения;

Потенциальные угрозы потери данных:

- потери при заражении системы компьютерными вирусами;
- потери связанные с несанкционированным доступом;
- потери информации связанные с неправильным хранением архивных данных;
- ошибки обслуживающего персонала и пользователей.

Способы защиты информации:

- **ПРЕПЯТСТВИЕ** – физически преграждает злоумышленнику путь к защищаемой информации;
- **УПРАВЛЕНИЕ ДОСТУПОМ** – способ защиты информации регулированием использования всех ресурсов системы (технических, программных средств, элементов данных);
- **РЕГЛАМЕНТАЦИЯ** – разработка мероприятий, создающих условия автоматизированной обработки и хранения в сети защищаемой информации;
- **ПРИНУЖДЕНИЕ** – соблюдение правил обработки и использования защищаемой информации пользователями и персоналом.

Физическая защита данных

- прокладка кабелей с использованием защищенных коробов;
- установка источников бесперебойного питания;
- организация сетевой инфраструктуры;
- установка активного оборудования в закрываемые шкафы;
- установка серверов в отдельном помещении с ограниченным доступом;
- установка и использование резервного питания.

Идентификация и ***аутентификация*** – основа программно – технических средств безопасности

Программно-технические средства защиты данных:

- средства управления доступом;
- ограничивающий интерфейс;
- шифрование данных.

Цели протоколирования и аудита:

- обеспечение подотчетности пользователей;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления анализа проблем.

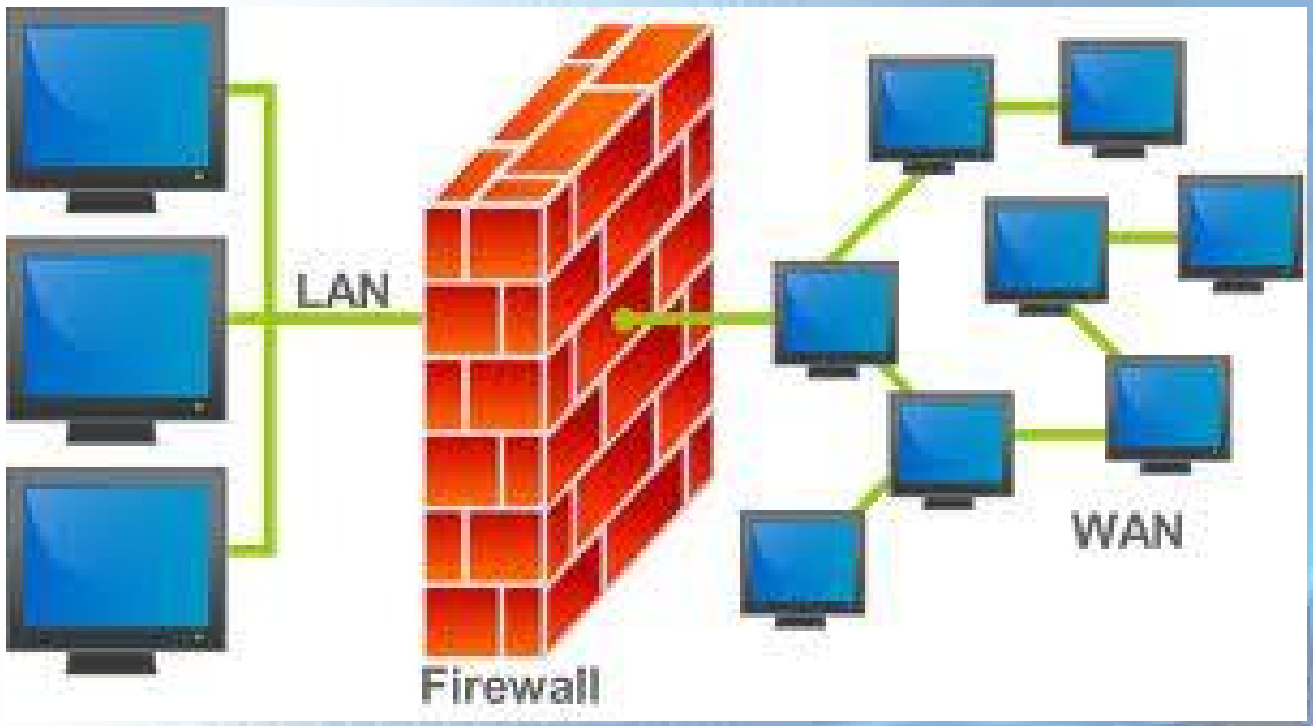
Архивация данных – важнейшая задача по обеспечению сохранности информации

Централизованное управление ЭВМ в библиотеке ДонГТУ.

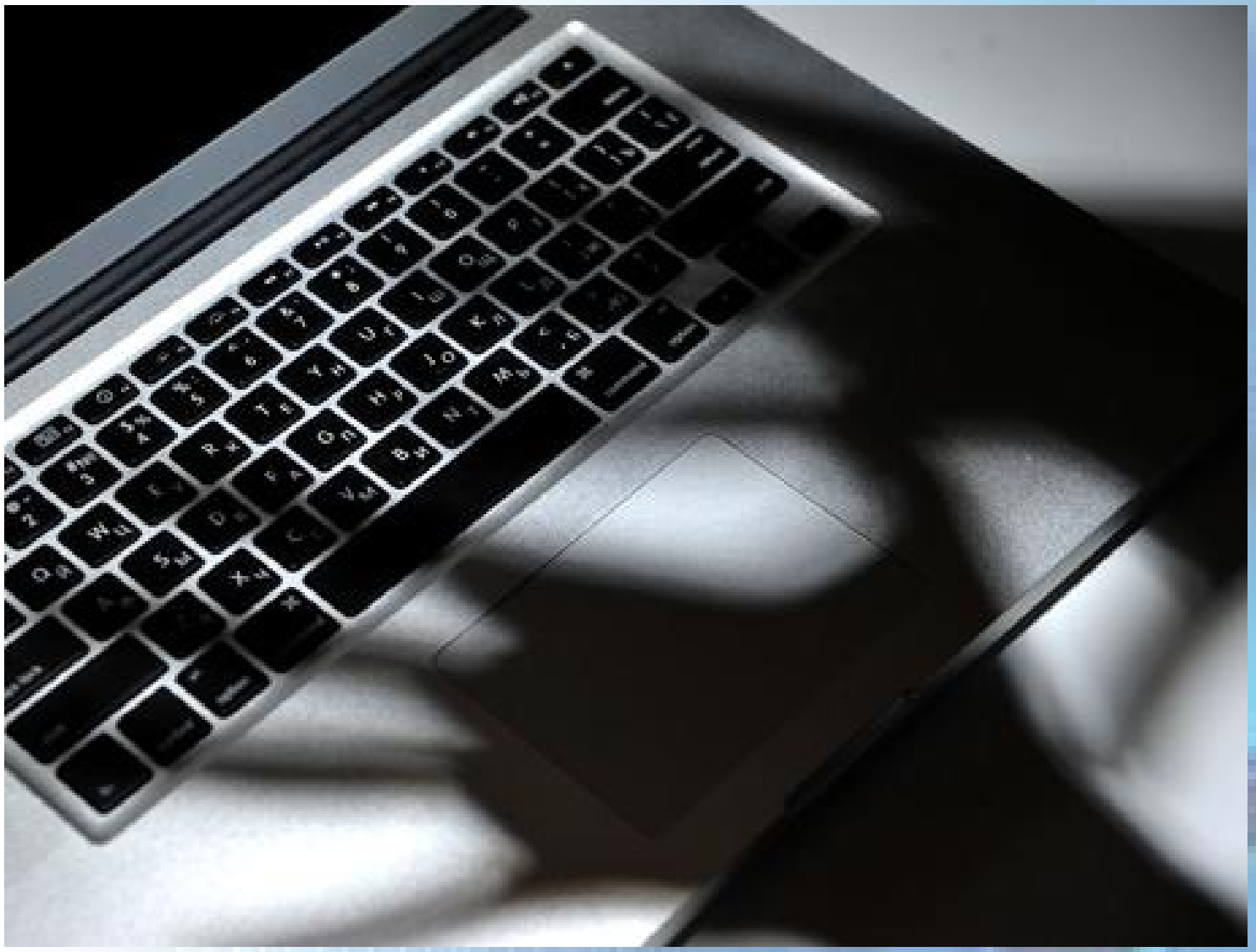
- Развертывание службы каталогов Active Directory;
- Учетные записи пользователей, с целью безопасности, ограничены в правах.
- Разработана и внедрена политика ограничения на запуск стороннего ПО в пределах домена.
- Регулярно и автоматически создается резервная копия системного диска рабочих мест.
- Рабочие места укомплектованы антивирусным ПО.
- Все пользователи проходят аутентификацию.

Экранирование

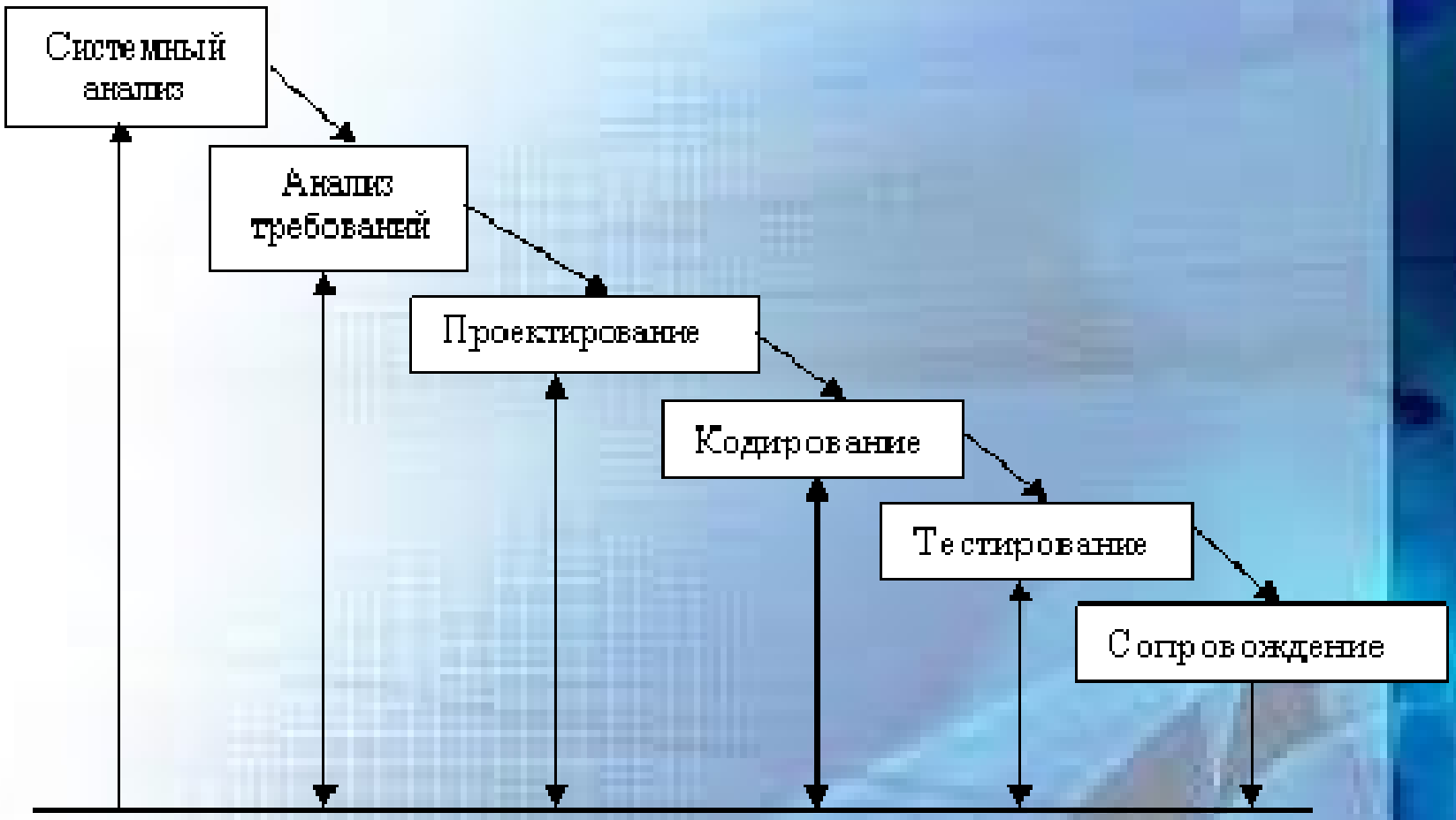
ЭКРАН (*фаерволл, брэндмауер*) – это средство разграничению доступа клиентов из одного множества к серверам из другого множества.



Безопасность web-ресурса



Этапы разработки web-ресурса



Меры безопасности:

- установлены настройки безопасности сервера;
- регулярно проводятся обновления программного обеспечения;
- аудит безопасности сервера и web – интерфейса;
- разграничены права пользователей.

Спасибо
за внимание