1 Безопасность

Корреляция - связанность между какими-либо признаками, при изменении одного признака - изменяются другие.

Безопасная компьютерная система – по средствам специальных механизмов защиты контролируется доступ к информации, таким образом, что только имеющие соответствующие полномочия лица или процессы, выполняющиеся от их имени, могут получить доступ на чтение, изменение, создание или удален

Аудит любой системы и найти к какому уровню безопасности соответствует

2 Уровни безопасности

CRUD
| D
| C
| B
| A

2.1 D

Система идентификации и аутентификации, подсистема подсчета событий, связанных с безопасностью и избирательный(дискреционный) контроль доступа

Идентификация – присвоение некоторых идентификаторов субъекту

- То что субъекту ... (пароль)
- То что субъекту принадлежит (номер телефона)
- То что является характеристикой субъекта (биометрия)

Аутентифакиция – сопоставление ...

Авторизация – назначение тех или иных прав доступа тому, кто прошел ауте

2.2 C

Дискреционный контроль доступа – в том или ином виде существует матрица субъект/объект, на пересечении - CRUD права

- Система имеет одного выделенного субъекта и только он имеет право устанавливать любые другие права

- Каждый объект системы имеет привязанного к себе 'владельца', который может назначать права доступа
- Субъект с определенным правом доступа может передать данное право другому субъекту

ACL - access control list

2.2.1 C1

Требование разделения пользователей и данных и определение контура обеспечения безопасности

Доверенная вычислительная база – совокупность защитных механизмов, включающих аппаратное ПО, отвечающих за проведение ... политики безопасности

Должны иметь средства проверки на то что контур безопасности работает корректно

2.2.2 C2

Журнал контроля доступа к системе, изоляция ресурсов

Изоляция ресурсов – при выделении объекта из определенного пула вычислительной базы, затем удаляются следы его использования

Проводится тестирование механизма ресурсов

2.3 B

Применение мандатного доступа(вместо дискреционного)

- Каждому объекту и субъекту ставится в соответствие 'метка секретности'
- Субъект может получать доступ на чтение объектов с его уровнем доступа или ниже
- Субъект имеет право на запись только в объекты со своим уровнем доступа или выше

2.3.1 B1

Мандатное управление доступа к выбранным субъктам и объектам

2.3.2 B2

Абсолютно любой объект и объект должны быть классифицированны и включены в систему управления мандатным доступом

2.3.3 B3

Включает B2 + выделение спецального домена безопасности

Домен характеризуется наличием специального администратора безопасности и системой ...

2.4 A

Все функции B3 + формализованные процедуры проектирования и распространения

3 Ролевая модель

Ролевая модель доступа – матрица строится относительно роль/субъект

Быстрая проверка по ACL ролей

4 Про безопасность

Аудит – пытаемся записывать все действия и по ним пытаемся вычислить наличие аномалий

Модели доступа помогают решать проблемы штатного доступа

Виды шифрования:

- *Прозрачное шифрование БД* – пока я работаю с данными в памяти - не шифрованный вид, на диске все данные зашифрованы

  Ключ - один на все

- *Шифрование на уровне столбцов* – для разных столбцов - разные ключи

  Необходимо передавать ключ, нет доступа к данным без ключа

- *Шифрование с тестами файловой системы* – при записи файловая система шифрует данные, а не БД

- *Шифрование на уровне приложений* – данные всегда в зашифрованном виде, шифруем на стороне приложения

  Проблемы с производительностью, надежностью

Всегда должен быть субъект с наивысшими правами доступа

Проблема разрешима через:

- Резервное копирование (через многоуровневые системы)

- Создание систем с невозможностью изменения данных