1. Что такое группы Active Directory? Типы групп.

Active Directory – службы каталогов корпорации Microsoft для операционных систем семейства Windows server. Первоначально создавалась как LDAP-совместимая реализация службы каталогов.

Существует три типа групп:

* Локальная
* Глобальная
* Универсальная

2. Перечислите политики паролей. Что они определяют?

* Минимальные и максимальные длины паролей
* Минимальные и максимальные сроки действия этих паролей
* Требования к сложности пароля
* Хранения паролей с помощью реверсируемого шифрования

3. Перечислите политики блокировки учетной записи. Что они определяют?

* Блокировка после некоторого количества неудачных попыток входа
* Время, на которое устанавливается блокировка
* Время, через которое сбрасывается счетчик неудачных входов

4. Что такое аудит? Перечислите политики аудита.

Аудит – процесс отслеживания различных действий, выполняемых ОС. Политики аудита объединены в группы:

* Аудит проверки учетных данных
* Аудит службы проверки подлинности Kerberos
* Аудит операций с билетами службы Kerberos
* Аудит других событий входа учетных записей
* Управление учетными записями
* Аудит управления группами приложений
* Аудит управления группами распространения
* Аудит других событий управления учетными записями
* Аудит управления группами безопасности
* Аудит управления учетными записями пользователей

5. Что содержит журнал событий безопасности?

Журнал событий безопасности содержит события, относящиеся к обеспечению безопасности системы.

* попытки входа в учетную запись
* использование ресурсов (файлов, реестра, устройств)
* управление учетными записями
* изменения прав и привилегий аккаунтов
* запуск и остановка процессов (программ)

Типы регистрируемых событий можно сконфигурировать с помощью редактора политик.