**Практическое задание по лекции 14**

**Вопросы лекция 14**

1. Из каких компонентов состоит система защиты ОС Windows?

2. Что в себя включает процедура регистрации (Logon Processes)?

3. Что является центральным компонентом системы защиты Windows NT?

4. Для чего предназначен менеджер учёта (Security Account Manager)?

5. Какую роль выполняет диспетчер доступа (Security Reference Monitor)?

6. Где хранится база данных Lsass? Что она содержит?

7. Каким требованиям отвечает система безопасности ОС Windows?

8. На какие вопросы подразумевает ответы политика безопасности?

9. Назовите требования, которые предъявляются к системе защиты.

10. Чем отличается ОС Windows от большинства операционных систем?

11. Чем обладает каждый пользователь, при ролевом доступе?

12. Каким образом представлена каждая привилегия?

13. Где перечислены привилегии и права учётных записей?

14. Назовите привилегии, которые вы знаете.

15. Почему администратор по умолчанию обладает не всеми привилегиями?

**Словарь лекция 14**

Система защиты ОС Windows - это набор компонентов для защиты целостности аппаратного и программного обеспечения.

Процедура регистрации (Logon Processes) - это компонент операционной системы Microsoft Windows, отвечающий за вход в систему.

Подсистема локальной авторизации (Local Security Authority) - это компонент операционной системы Windows, отвечающий за авторизацию локальных пользователей отдельного компьютера.

Маркер доступа - программный объект операционных систем класса Microsoft Windows, содержит информацию по безопасности сеанса и идентифицирует пользователя, группу пользователей и пользовательские привилегии.

Локальная политика безопасности - это набор сведений о безопасности локального компьютера. Сведения о локальной политике безопасности включают в себя следующее: Домены, доверенные для проверки подлинности попыток входа. Какие учетные записи пользователей могут получить доступ к системе и как.

Политика аудита - это то, что определяет, следует ли выполнять аудит при перезапуске или выключении компьютера пользователем или при возникновении события, влияющего на безопасность системы или журнал безопасности.

Lsasrv.dll - файл, в котором реализована основная часть функциональности подсистемы локальной авторизации.

Менеджер учета (Security Account Manager) - это компонент операционной системы, который управляет базой данных учета пользователей.

Диспетчер доступа (Security Reference Monitor) - это компонент операционной системы, отвечающий за проверку пользовательских прав на доступ к объекту и на выполнение тех действий, которые он пытается совершить.

Common Criteria - принятый в России международный стандарт по компьютерной безопасности.

Luid - это внутренний номер привилегии в конкретной системе.

MS Platform SDK - это комплект разработки программного обеспечения от Microsoft, который содержат файлы заголовков, библиотеки, примеры, документацию и инструменты, необходимые для разработки приложений для Microsoft Windows.

WinNT.h - это файл, содержащий перечень привилегий.

NTSecAPI.h - это файл, содержащий перечень прав.

Назначение и отзыв привилегий - прерогатива локального администратора безопасности LSA (Local Security Authority), поэтому, чтобы программно назначать и отзывать привилегии, необходимо применять функции LSA.

PolicyHandle - это описатель объекта политики, который необходимо получить при использовании функции LSA, при помощи функции LsaOpenPolicy, которая открывает описатель объекта на локальной или удаленной машине.

LsaEnumerateAccountRights - это функция, которая перечисляет привилегии пользователя с заданным идентификатором безопасности Sid в отношении системы с объектом политики PolicyHandle, передаваемыми ей в качестве параметров.

LsaAddAccountsRights и LsaRemoveAccountRights - это функции добавления и отзыва привилегий соответственно.

Функция LookupPrivilegeDisplayName - это функция, которая преобразует программное имя привилегии в дружественное имя.

Функция CharToOem - это функция, которую используют для вывода имени привилегии на экран на русском языке.