Практическое задание по лекции №14

Из каких компонентов состоит система защиты windows?

Какому классу из «оранжевой» книги соответствует система безопасности windows

Кто такие администраторы в системе windows?

Опишите различие между привилегиями и разрешениями?

С помощью какого API можно формировать список привилегий?

Какие проблемы у перечисления привилегий учетной записи?

Какой функцией можно назначить привилегии?

Сколько текстовых представлений имеет привилегия?

Чем занимается подсистема локальной авторизации?

Расскажите о диспетчере доступа ?

Процедура регистрации (Logon Processes), которая обрабатывает запросы пользователей на вход в систему

Подсистема локальной авторизации (Local Security Authority, LSA), которая гарантирует, что пользователь имеет разрешение на доступ в систему.

Менеджер учета (Security Account Manager, SAM), который управляет базой данных учета пользователей

Диспетчер доступа (Security Reference Monitor, SRM), проверяющий, имеет ли пользователь право на доступ к объекту и на выполнение тех действий, которые он пытается совершить

С целью гибкого управления системной безопасностью в ОС Windows реализовано управление доверительными отношениями (trusted facility management), которое требует поддержки набора ролей (различных типов учетных записей) для разных уровней работы в системе.

В системе имеется управление привилегированным доступом, то есть функции администрирования доступны только одной группе учетных записей - Administrators (Администраторы.).

Назначение и отзыв привилегий - прерогатива локального администратора безопасности LSA

Управление привилегиями пользователей включает в себя задачи перечисления, задания, удаления, выключение привилегий и ряд других

Привилегии перечислены в файле WinNT.h, а права - в файле NTSecAPI.h из MS Platform SDK.

Все компоненты активно используют базу данных Lsass, содержащую параметры политики безопасности локальной системы, которая хранится в разделе HKLM\SECURITY реестра.