Практическое задание по лекции №13

Для построения формальных моделей безопасности в виде каких сущностей принято представлять ИС?

Каким ещё доступом кроме дискреционного windows поддерживает управление?

чем обеспечивается единообразие контроля доступа к различным объектам?

Что содержит учётная запись пользователя?

Как можно создать учётную запись?

В каком виде система хранит идентификаторы безопасности?

Каких двух типов есть записи ACE в списке ACL?

Назовите основные этапы проверки прав доступа

Что такое ролевая политика безопасности?

Что такое дискреционная модель контроля?

Сущность, от которой нужно защищать объекты, называется "субъектом". Субъектами в Windows являются процессы и потоки, запускаемые конкретными пользователями. Субъект безопасности - активная системная составляющая, а объект – пассивная

Основной вывод из анализа применяемых в ОС Windows моделей контроля доступа (комбинация дискреционной и ролевой): нельзя формально обосновать безопасность ИС в случаях, представляющих практический интерес.

Ключевая цель системы защиты Windows - следить за тем, кто и к каким объектам осуществляет доступ

И каждый пользователь и каждая группа пользователей системы должны иметь учетную запись (account) в базе данных системы безопасности

SID пользователя (и группы) является уникальным внутренним идентификатором и представляют собой структуру переменной длины с коротким заголовком, за которым следует длинное случайное число.

В ОС Windows все типы объектов защищены одинаковым образом. С каждым объектом связан дескриптор защиты (security descriptor).

Очевидно, что для процедуры проверки важен порядок расположения ACE в DACL. Поэтому Microsoft предлагает так называемый предпочтительный порядок размещения ACE. Например, для ускорения рекомендуется размещать запрещающие элементы перед разрешающими.

Представление информационной системы как совокупности взаимодействующих сущностей - субъектов и объектов - является базовым представлением большинства формальных моделей.

Можно ввести также особый вид субъекта, который активизируется при каждом доступе и называется монитором обращений. Если монитор обращений в состоянии отличить легальный доступ от нелегального и не допустить последний, то такой монитор называется монитором безопасности (МБ) и является одним из важнейших компонентов системы защиты.

Другая возможность, предоставляемая ОС Windows - управление ролевым, в частности привилегированным доступом.