**Практическое задание по лекции 13**

**Вопросы лекция 13**

1. В виде совокупности, каких взаимодействующих сущностей принято представлять ИС для построения формальных моделей безопасности?

2.Что включают в себя защищаемые объекты Windows?

3. Что является субъектами в Windows?

4. Как называется активная системная составляющая?

5. Как называется пассивная системная составляющая?

6. Как называется стратегия, при которой пользователь, как член группы, имеет набор полномочий, необходимых для его деятельности, и играет определенную роль?

7. В каких случаях нельзя формально обосновать безопасность ИС?

8. Какая ключевая цель системы защиты Windows?

9. Что требует модель защиты ОС Windows?

10. Что такое значение SID?

11. Какие 2 типа записи ACE есть в списке ACL?

**Словарь лекция 13**

Субъект - это сущность, от которой нужно защищать объекты.

Управление привилегированным доступом - это часть общей концепции управления доступом, направленная на сопровождение и контроль работы пользователей с расширенными правами.

POSIX - это набор стандартов, описывающих интерфейсы между операционной системой и прикладной программой, библиотеку языка C и набор приложений и их интерфейсов.

API - это механизмы, которые позволяют двум программным компонентам взаимодействовать друг с другом, используя набор определений и протоколов.

WhoAmI.exe - это результат отсутствия или повреждения версий исполняемого файла.

cacls.exe - это утилиты управления доступом.

ShowACLs.exe - это полезная утилита командной строки. С ее помощью можно отобразить разрешения на доступ к файлам и папкам на разделах NTFS, в том числе разрешения доступа пользователей.

SubInACL - это утилита командной строки, которая позволяет администраторам получать информацию о безопасности файлов, ключей реестра и служб, и переносить эту информацию от одного пользователя к другому, из одной группы (локальной или глобальной) в другую, из домена в домен.

PuList.exe - это утилита, которая предоставляет список процессов, запущенных на локальной или удаленной системе, их идентификаторов процессов (PID) и контекстов защиты для каждого процесса.

Security Account Manager - RPC-сервер Windows, оперирующий базой данных учетных записей. SAM выполняет следующие задачи: Идентификация субъектов; Проверка пароля, авторизация; Хранит статистику; Хранит настройки политики учетных записей и приводит их в действие.

HKLM/SAM - это данные, используемые для диспетчера учетных записей Security Accounts Manager (SAM), которые недоступны через редакторы реестра.

SID (SecurityIDentifier) - это структура данных переменной длины, которая идентифицирует учётную запись пользователя, группы, службы, домена или компьютера. SID ставится в соответствие каждой учётной записи в момент её создания.

Net-функции - это функции, благодаря которым можно управлять учетными записями пользователей, как на локальной, так и на удаленной системе.

Дескриптор безопасности - дескриптор, который содержит сведения о безопасности, связанные с защищаемым объектом.

ACL - это список управления доступом, который определяет, кто или что может получать доступ к объекту.

SACL - это список управления доступом к объектам «Microsoft Windows», используемый для аудита доступа к объекту.

Access Control Entry - это элемент в списке управления доступом (ACL).

DACL (Discretionary Access Control List ) - список избирательного управления доступом, контролируемый владельцем объекта и регламентирующий права пользователей и групп на действия с объектом.

Компиляция - трансляция программы, составленной на исходном языке высокого уровня, в эквивалентную программу на низкоуровневом языке, близком машинному коду (абсолютный код, объектный модуль, иногда на язык ассемблера), выполняемая компилятором.

SetTokenInformation - это функция, которая задает различные типы сведений для указанного маркера доступа.

GetTokenInformation - это функция, которая извлекает указанный тип сведений о маркере доступа.