Лекция 13
Система управления доступом

Практическое задание по лекции

Используя учебный материал лекции, составьте терминологический словарь, состоящий по объему из 20 терминов и определений.

1. Учетная запись (account): Учетная запись представляет собой запись в базе данных системы безопасности, которая идентифицирует пользователя или группу пользователей.
2. Привилегии пользователя (user privileges): Привилегии пользователя определяют разрешения и возможности, которыми обладает пользователь в системе.
3. Идентификатор безопасности (SID, Security Identifier): Идентификатор безопасности (SID) - это уникальный идентификатор, который присваивается каждой учетной записи в операционной системе Windows.
4. Группа пользователей (user group): Группа пользователей - это совокупность учетных записей пользователей, которые объединяются вместе для упрощения администрирования и назначения привилегий.
5. Win32-функция NetUserAdd: NetUserAdd - это функция, входящая в семейство сетевых функций операционной системы Windows.
6. Утилита getsid: Getsid - это утилита в операционной системе Windows, которая также позволяет пользователям получить информацию о своей учетной записи и идентификаторе безопасности (SID).
7. Функция LookupAccountSid: LookupAccountSid - это функция в операционной системе Windows, которая используется для получения имени пользователя или группы на основе заданного идентификатора безопасности (SID).
8. Дескриптор защиты (Security Descriptor): Дескриптор защиты (Security Descriptor) - это структура типа SECURITY_DESCRIPTOR в операционной системе Windows, которая описывает права доступа и аудита для конкретного объекта.
9. Контроль доступа (Access Control): Контроль доступа (Access Control) - это механизм в операционной системе Windows, который определяет, какие операции процессы или пользователи могут выполнять с объектом.
10. Список системного контроля доступа (SACL, System ACL): Список системного контроля доступа (SACL) - это часть дескриптора защиты объекта, аналогичная списку контроля доступа (DACL).

11. Маркер доступа (Access Token): Структура данных, содержащая информацию о контексте пользователя, привилегиях, группах и параметрах сессии.
12. Учетная запись (Account): Запись, содержащая информацию о пользователе или группе в операционной системе.
13. Список DACL (Discretionary Access Control List): Список, хранящийся в маркере доступа или дескрипторе защиты объекта, содержащий записи ACE (Access Control Entry).
14. Стандартная защита (Default Protection): Защита, которая применяется к объектам, если явные атрибуты безопасности не указаны субъектом.
15. Проверка прав доступа (Access Checking): Процесс сопоставления прав субъекта с правами доступа, указанными в списке DACL объекта.
16. Дискреционная модель управления доступом: Модель управления доступом, в которой обычные пользователи могут принимать участие в определении политики доступа и присвоении атрибутов безопасности.
17. Матрица доступа: Концептуальное представление текущего состояния прав доступа в дискреционной модели управления доступом.
18. Критерий Харрисона-Руззо-Ульмана: Критерий безопасности, утверждающий, что для обеспечения безопасности системы в начальном состоянии не должно существовать последовательности команд, которые добавляют право доступа в матрицу доступа, если оно отсутствовало в начальном состоянии.
19. Каналы утечки информации: Механизмы, которые позволяют несанкционированно раскрыть информацию из системы. В системах с дискреционным доступом возможны различные каналы утечки, такие как переброска информации в доступные объекты или создание скрытых каналов через программные ошибки.
20. Ролевая политика безопасности: Модель управления доступом, основанная на назначении ролей пользователям и определении прав доступа для каждой роли.