Лекция 14
Структура системы защиты. Привилегии

Практическое задание по лекции

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

1. Discretionary Access Control: Система контроля доступа, которая позволяет владельцам ресурсов определять права доступа для других пользователей или групп пользователей.
2. Logon Processes: Механизм, отвечающий за обработку запросов пользователей на вход в систему.
3. Security Account Manager: Компонент, отвечающий за управление базой данных учета пользователей в системе.
4. Security Reference Monitor: Компонент, который проверяет, имеют ли пользователи право на доступ к объектам и выполнение требуемых действий.
5. Authentication: Процесс проверки подлинности пользователя или системы для доступа к ресурсам или функциональности.
6. Access Management: Процесс управления разрешениями на доступ к ресурсам или функциям системы.
7. Role Sets: Наборы ролей или различных типов учетных записей, которые поддерживаются в системе.
8. Security Audit: Процесс регистрации и учета событий, связанных с безопасностью системы, в целях контроля и обнаружения потенциальных угроз или нарушений безопасности.
9. Privileged Access Management: Процесс управления и контроля доступа к привилегиям в системе.
10. Permission: Право или разрешение, предоставляемое пользователям или ролям для доступа к конкретным объектам или ресурсам в системе.
11. Account Group: Совокупность учетных записей пользователей, объединенных по схожим характеристикам или требованиям доступа.
12. Principle of Least Privilege: Принцип безопасности, согласно которому каждый пользователь или процесс должен обладать только теми привилегиями, которые необходимы для выполнения своих задач.

13. Privilege: Специальное право, которое предоставляется пользователю или группе пользователей в операционной системе Windows.
14. Local Security Authority: Локальный Авторитет Безопасности (Local Security Authority) - компонент операционной системы Windows, отвечающий за управление политикой безопасности, включая назначение и отзыв привилегий.
15. Security Policy Object: Объект, который содержит информацию о политике безопасности системы, включая информацию о привилегиях пользователей, правах доступа и других атрибутах безопасности.
16. LsaEnumerateAccountRights: Функция в API LSA, используемая для перечисления привилегий, назначенных конкретной учетной записи пользователя.
17. Маркер доступа (Access Token): Структура данных, содержащая информацию о безопасности пользователя, включая его идентификатор безопасности (SID), привилегии, группы, к которым он принадлежит, и другие атрибуты.
18. LsaAddAccountRights: Функция в API LSA, используемая для назначения одной или нескольких привилегий конкретной учетной записи пользователя.
19. LsaRemoveAccountRights: Функция в API LSA, используемая для отзыва одной или нескольких привилегий учетной записи пользователя.
20. SE_SHUTDOWN_NAME: Конкретная привилегия, которая позволяет пользователю завершать работу операционной системы, выключать компьютер или перезагружать его.