

**Темы для подготовки к дифференцированному зачету по МДК.01.01
«Эксплуатация подсистем безопасности автоматизированных систем»
5 семестр**

Теоретические вопросы

- 1 Определение аутентификация, протоколирование, аудит
- 2 Подсистема безопасности в операционных системах (база данных SAM, идентификатор безопасности, маркер доступа, SID пользователя, служба LSA, UID, GID, EUID, EGID, вектор доступа, PAM и т. д.)
- 3 Методы доступа (дискреционный, полномочный, мандатный метод, матрица доступа и т.д.)
- 4 Система разграничения доступа к информации
- 5 Права доступа в UNIX (rwx)
- 6 Права доступа в Windows (специальные, стандартные, общие)
- 7 Параметры парольной аутентификации
- 8 Протоколирование и аудит, механизм аудита
- 9 Методы предвыбора событий аудита, поствыбора событий аудита. Недостатки и достоинства
- 10 Аудит в операционной системе Windows. Системный журнал, журнал приложений, журнал безопасности

Практические задания

- Создать пользователя с ограниченными правами. Присвойте идентификатор созданному пользователю (в качестве идентификатора используйте сменный носитель информации). Задайте указанный уровень допуска полномочного управления.
- Установить следующие параметры:
 - максимальный срок действия ключа
 - локальное оповещение об НСД
 - количество неудачных попыток аутентификации
 - реакция на изъятие идентификатора
 - режим аутентификации пользователя
 - режим идентификации пользователя
 - параметры затирания данных
 - параметры обработки при контроле печати маркированных документов
 - уровни конфиденциальности
- Создайте папку «Документы», содержащую три документа с заданными уровнями конфиденциальности. Например, Документ1.txt (уровень конфиденциальности — Неконфиденциально), Документ2.txt (уровень конфиденциальности — Конфиденциально), Документ3.txt (уровень конфиденциальности — Для бухгалтерии)
- Настроить контроль целостности данных для заданного объекта, установив указанные метод контроля и реакцию системы