Практическая работа №13

*Выполнил Шардт М.А.*

1. Задание 1
   1. Какие важные элементы содержат учетные записи пользователей?
   2. Какие действия необходимо выполнить для успешного применения Net-функций?
   3. Какое инструментальное средство в операционной системе Windows используется для управления учетными записями пользователей?
   4. Какую информацию можно получить с помощью утилиты WhoAmI.exe?
   5. Какие утилиты можно использовать для просмотра и редактирования списков контроля доступа?
   6. Что такое SID?
   7. Где хранятся учетные записи пользователей в операционной системе?
   8. Какая структура данных используется для передачи информации о создаваемой учетной записи пользователя в Net-функциях?
   9. Зачем субъектам контекст пользователя?
   10. Что такое субъект безопасности?
2. Задание 2
   1. Субъект – сущность, от которой нужно защищать объекты
   2. Контекст пользователя – отличительные признаки субъекта
   3. Роль – свойства, которые ставятся каждому субъекту и тем объектам, которые он использует
   4. Дескриптор защиты – специальный атрибут объекта, содержащий информацию обо всех пользователях, которым разрешен или запрещен доступ к объекту
   5. Маркер доступа – программный объект операционных систем класса Microsoft Windows, содержит информацию по безопасности сеанса и идентифицирует пользователя, группу пользователей и пользовательские привилегии
   6. Контроль привилегированных пользователей – это комплекс решений, который помогает осуществлять мониторинг и контроль учётных записей, а также аудит выполняемых действий
   7. Учётная запись – хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам
   8. Управление доступом на основе ролей – развитие политики избирательного управления доступом, при этом права доступа субъектов системы на объекты группируются с учётом специфики их применения, образуя роли
   9. Избирательное управление доступом – управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа
   10. SAM – RPC-сервер Windows, оперирующий базой данных учетных записей
   11. SID – это уникальный идентификатор, который присваивается пользователям, группам, компьютерам или другим объектам безопасности при их создании в Windows или Active Directory
   12. Net-функции – семейство сетевых функций ОС Windows
   13. DACL – список избирательного управления доступом, контролируемый владельцем объекта и регламентирующий права пользователей и групп на действия с объектом
   14. SACL – список управления доступом к объектам Microsoft Windows, используемый для аудита доступа к объекту
   15. ACE – запись управления доступом, которая определяет способ взаимодействия SID с защищаемым объектом. Может разрешать или запрещать доступ для определенного SID
   16. Монитор безопасности – монитор обращений, способный отличить легальный доступ от нелегального и не допустить последний
   17. Суперпользователь – это специальный аккаунт и группа пользователей в UNIX-подобных системах с идентификатором UID 0, владелец которого имеет право на выполнение всех без исключения операций
   18. Утилита – вспомогательная компьютерная программа в составе общего программного обеспечения для выполнения специализированных типовых задач, связанных с работой оборудования и операционной системы
   19. Домен Windows NT – собрание участников безопасности, имеющих единый центр, использующий единую базу, известную как Active Directory
   20. Формальная модель – представление концептуальной модели с помощью одного или нескольких формальных языков