Практическая работа №14

*Выполнил Шардт М.А.*

1. Задание 1
   1. Какие компоненты входят в систему безопасности?
   2. Что такое монитор безопасности и как он связан с моделью дискреционного контроля доступа?
   3. Какие требования предъявляются к системе защиты?
   4. Какие компоненты системы защиты ответственны за управление политикой безопасности и базой данных учета пользователей?
   5. Что такое привилегии ви как они назначаются?
   6. Чем отличаются привилегии и разрешения?
   7. Что такое Trusted Facility Management в ОС Windows и как он связан с управлением привилегиями?
   8. Какие функции доступны только группе учетных записей Administrators?
   9. Какую базу данных активно используют компоненты защиты ОС Windows?
   10. Что содержит база данных Lsass?
2. Задание 2
   1. Система контроля дискреционного доступа - центральная концепция защиты операционной системы Windows, которая определяет права доступа к объектам и ресурсам системы на основе настроек безопасности и идентификации пользователя.
   2. Монитор безопасности - особый вид субъекта, который активизируется при каждом доступе и в состоянии отличить легальный доступ от нелегального и не допустить последний. Входит в состав диспетчера доступа (SRM), который, согласно описанию, обеспечивает также управление ролевым и привилегированным доступом.
   3. Политика безопасности - задача, определяющая, какую информацию защищать, какого рода атаки на безопасность системы могут быть предприняты, какие средства использовать для защиты каждого вида информации. В системе безопасности операционной системы Windows политика безопасности подразумевает выполнение определенных требований, таких как поддержка уникальных идентификаторов пользователей, контроль доступа к ресурсам и т.д.
   4. Нормативный подход - методика оценки степени защищенности операционных систем, в соответствии с которой совокупность задач, решаемых системой безопасности, должна удовлетворять определенным требованиям, перечень которых определяется общепринятыми стандартами.
   5. Привилегия - право на выполнение определенных операций в отношении системы в целом или конкретных объектов. Привилегии назначаются администраторами отдельным пользователям или группам как часть настроек безопасности.
   6. Разрешение - право на выполнение определенных операций в отношении конкретных объектов. Разрешения назначаются администраторами отдельным пользователям или группам как часть настроек безопасности.
   7. Trusted Facility Management - механизм управления доверительными отношениями в ОС Windows, который требует поддержки набора ролей для разных уровней работы в системе.
   8. Administrators - группа учетных записей, которая имеет привилегированный доступ и функции администрирования в ОС Windows.
   9. LSA (Local Security Authority) - локальный администратор безопасности, который имеет прерогативу назначать и отзывать привилегии в системе.
   10. PolicyHandle - описатель объекта политики, который используется при управлении привилегиями пользователей в ОС Windows.
   11. Процедура регистрации – процедура, которая обрабатывает запросы пользователей на вход в систему
   12. Аутентификация – процедура проверки подлинности
   13. Подсистема локальной авторизации – процедура, которая гарантирует, что пользователь имеет разрешение на доступ в систему
   14. Инициализация – приведение цифрового устройства или его программы в состояние готовности к использованию
   15. Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определенными критериями и показателями безопасности
   16. Перекрёстная проверка – метод оценки аналитической модели и ее поведения на независимых данных. При оценке модели имеющиеся в наличии данные разбиваются на k частей. Затем на k−1 частях данных производится обучение модели, а оставшаяся часть данных используется для тестирования
   17. Маркер – специальный знак, наносимый на машинный носитель информации для выполнения служебной функции, обеспечивающей обработку информации
   18. Идентификаторы – имена, использующиеся для переменных, функций, меток и других определяемых пользователем объектов
   19. Пользователь – лицо или организация, которое использует действующую систему для выполнения конкретной функции
   20. База данных – это совокупность данных, которая включает в себя определенные правила, принципы хранения, описания и управления данными