МДК 03.01 Техническая защита информации

Теоретические вопросы:

1. Основные угрозы технической защиты информации.
2. Уровни целостности данных.
3. Утечки информации. Классификация
4. Технические каналы утечки информации
5. Средства и системы для обнаружения утечки информации
6. Концепции сниффинга
7. SQL Injection1221
8. Боты
9. Концепции рекогносцировки. Методология сбора информации
10. Атаки типа “Отказ в обслуживании”
11. Способы подавления опасных электрических сигналов акустоэлектрических преобразователей
12. Средства перехвата аудиоинформации
13. Направленные микрофоны
14. Диктофоны
15. Методы и устройства высокочастотного навязывания и средства защиты
16. Оптические средства добывания информации
17. Перехват информации в линиях связи
18. Перехват сообщений в каналах сотовой связи
19. Получение информации в компьютерных сетях
20. Методы и средства выявления закладных устройств
21. Технические средства защиты информации
22. Технические средства пространственного и линейного зашумления
23. Криптографические методы и средства защиты
24. Общие принципы организации защиты объектов
25. Классификация предметов защиты и объектов охраны
26. Классификация нарушителей и потенциальных угроз безопасности
27. Условия функционирования систем безопасности
28. Средства сбора, обработки, отображения информации и управления
29. Зоны обеспечения безопасности
30. Интегрированные комплексные системы безопасности. Классификация. Принципы организации. Структурные схемы
31. Устройства видеозаписи (видеорегистраторы)
32. Источники видеосигнала (видеокамеры)
33. Системы охранной, тревожной и пожарной сигнализации
34. Системы контроля и управления доступом
35. Телевизионные системы безопасности

36. Проектирование систем безопасности
37. Жизненный цикл систем безопасности
38. Методы оценки эффективности систем безопасности
39. Межсайтовый скриптинг
40. Компьютерные вирусы. Классификация
41. Техническая защита информации
42. Основные цели технической защиты информации.
43. Преимущества обеспечения безопасности сетевых соединений с помощью виртуальных частных сетей (vpn).
44. Защита от атак по сети и её важность.
45. Методы защиты от атак по сети
46. Основные меры безопасности информации от угроз в реальном времени.
47. Методы аутентификации для проверки подлинности пользователя.
48. Принципы безопасности, обеспечивающие аутентификацию и авторизацию пользователей.
49. Виды инженерно-технической защиты.
50. Общие положения защиты информации техническими средствами.

Практические задания:

1. Выявить и описать потенциальные каналы утечки информации в помещениях. Указать причины возникновения. Составить модель каналов утечки информации.
2. Для помещений определить основные источники информации и их носители. Классифицируйте и опишите категории помещений.
3. Представьте основные варианты возможной утечки речевой информации из объемов выделенных помещений. Определите группы и виды каналов утечки. Опишите технические средства, с помощью которых может быть осуществлен перехват информации. Опишите возможные каналы утечки информации.
4. Для объекта защиты составьте список потенциальных угроз безопасности.
5. Составьте план защиты объекта с помощью технических средств. Поясните расположение и обоснуйте свой выбор.
6. Настройка межсетевого экрана (firewall). Настройте межсетевой экран для защиты локальной сети от внешних атак. Заблокируйте входящие соединения на порты 22 (SSH) и 80 (HTTP), кроме разрешенных IP-адресов
7. Настроить межсетевой экран Windows для запрета входящих соединений на порты TCP 22 (SSH), UDP 53 (DNS), кроме разрешённых IP-адресов.
8. Анализ журнала событий Windows. Откройте журнал событий Windows и найдите последние 10 ошибок системы. Проанализируйте их и предложите меры по устранению.
9. Шифрование диска BitLocker. Зашифруйте системный диск с помощью BitLocker и настройте его для использования PIN-кода при загрузке.
10. Тестирование на проникновение (penetration testing). Проведите тестирование на проникновение локального веб-сервера с использованием Metasploit. Найдите и опишите хотя бы одну уязвимость.
11. Настройка VPN-соединения. Настройте VPN-сервер на Windows Server и подключитесь к нему с клиентского компьютера. Проверьте работоспособность туннеля.
12. Анализ сетевого трафика с помощью Wireshark Запустите Wireshark и захватите трафик HTTP-запроса к сайту. Проанализируйте захваченные пакеты и найдите запрос и ответ.
13. Создание зашифрованного контейнера VeraCrypt. Создайте зашифрованный контейнер с помощью VeraCrypt и поместите в него несколько файлов. Покажите процесс монтирования и демонтирования контейнера.
14. Настройка политики безопасности Windows. Создайте новую политику безопасности в Windows, которая запрещает запуск определенных приложений и устанавливает ограничения на доступ к файлам.
15. Анализ логов системы безопасности. Откройте логи системы безопасности Windows и найдите последние 10 событий входа в систему. Проанализируйте их и определите, были ли неудачные попытки входа.
16. Настройка двухфакторной аутентификации. Настройте двухфакторную аутентификацию для учетной записи Microsoft с использованием мобильного приложения-аутентификатора.
17. Анализ уязвимостей с помощью Nmap. Проведите сканирование сети с использованием Nmap и найдите открытые порты и уязвимости на одном из хостов.

18. Настройка антивирусного ПО.Установите и настройте антивирусное ПО (например, Kaspersky Endpoint Security) на рабочем компьютере. Проведите полное сканирование системы.
19. Анализ конфигурации брандмауэра Windows. Откройте настройки брандмауэра Windows и проанализируйте текущие правила. Создайте новое правило, которое блокирует исходящий трафик на определенный IP-адрес.
20. Зашифровать системный диск с помощью BitLocker, настроить защиту с помощью PIN-кода и сохранить ключ восстановления в безопасный сетевой ресурс.
21. Создать локальную политику безопасности, запретив запуск определённых приложений и установив ограничения на доступ к критически важным папкам.
22. Проанализировать логи системы безопасности Windows и выявить последние 5 попыток несанкционированного доступа. Предложить меры защиты.
23. Создать простую веб-страницу с формой авторизации и реализовать защиту от SQL-инъекций с применением параметризованных запросов.
24. Создать полную резервную копию системы с помощью встроенных средств Windows. Восстановить систему на виртуальной машине.
25. Настроить расписание инкрементального резервного копирования файлов и папок с помощью PowerShell.