**Экзаменационные вопросы Анализ безопасности ОС**

1. Опишите основные методы защиты операционных систем и их роль в обеспечении безопасности данных.
2. Дайте понятие антивирусного программного обеспечения и охарактеризуйте его основные функции в защите операционной системы.
3. Перечислите уровни защиты операционных систем и объясните, как они взаимодействуют друг с другом.
4. Охарактеризуйте механизмы контроля доступа в операционных системах и их значение для предотвращения несанкционированного доступа.
5. Раскройте особенности использования системного журнала и мониторинга событий для защиты операционных систем.
6. Охарактеризуйте основные виды угроз, существующих в операционных системах, и их влияние на безопасность данных.
7. Дайте понятие уязвимости операционных систем и объясните, как они могут быть использованы злоумышленниками.
8. Опишите различия между внутренними и внешними угрозами для операционных систем, приведя примеры.
9. Перечислите основные способы реализации вредоносного программного обеспечения в операционных системах и охарактеризуйте их последствия.
10. Раскройте особенности социальных атак на пользователей операционных систем и их связь с нарушением безопасности.
11. Опишите процесс настройки автозапуска служб в Windows 10/11 и его влияние на производительность системы.
12. Дайте понятие службы Windows и охарактеризуйте их роль в обеспечении работы операционной системы.
13. Перечислите основные методы управления службами в Windows 10/11 и объясните их функциональное назначение.
14. Охарактеризуйте параметры служб Windows 10/11 (вручную, автоматически, отключено) и их применение в различных сценариях.
15. Раскройте особенности настройки служб для повышения безопасности и оптимизации работы Windows 10/11.
16. Опишите ключевые особенности файловой системы NTFS и охарактеризуйте её преимущества по сравнению с FAT.
17. Дайте понятие файловой системы FAT и объясните её основные характеристики и ограничения.
18. Перечислите основные различия между файловыми системами NTFS и FAT в контексте их применения в Windows 10/11.
19. Охарактеризуйте механизм управления правами доступа в файловой системе NTFS и его влияние на безопасность данных.
20. Раскройте особенности поддержки больших файлов и разделов в NTFS и FAT, а также их значение для современных операционных систем.
21. Опишите процесс настройки автоматического создания резервных копий в Windows 10/11 и его значение для защиты данных.
22. Дайте понятие резервного копирования операционной системы и охарактеризуйте основные методы его реализации в Windows 10/11.
23. Перечислите доступные инструменты Windows 10/11 для резервного копирования данных и объясните их функциональные особенности.
24. Охарактеризуйте процесс восстановления системы из резервной копии и его роль в обеспечении отказоустойчивости.
25. Раскройте основные рекомендации по управлению резервными копиями для минимизации потерь данных и оптимизации использования дискового пространства.
26. Опишите основные принципы обеспечения безопасности в ОС Linux и их влияние на защиту данных.
27. Дайте понятие ролевой модели безопасности в Linux и охарактеризуйте её применение в системе.
28. Перечислите ключевые инструменты и утилиты Linux для управления безопасностью и объясните их назначение.
29. Охарактеризуйте механизм управления правами доступа к файлам и каталогам в Linux и его значение для защиты системы.
30. Раскройте особенности настройки брандмауэра в Linux и его роль в обеспечении сетевой безопасности.
31. Опишите процесс настройки сетевых адаптеров в Windows 10/11 и Linux, указав их основные параметры.
32. Дайте понятие сетевого интерфейса и охарактеризуйте его управление через командные утилиты в Linux и графические интерфейсы Windows 10/11.
33. Перечислите основные команды и утилиты для диагностики сетевых подключений в Linux и Windows 10/11, объяснив их назначение.
34. Охарактеризуйте процесс настройки IP-адреса и других сетевых параметров в Windows 10/11 и Linux, указав отличия в подходах.
35. Раскройте особенности управления беспроводными сетями в Linux и Windows 10/11, включая подключение, диагностику и устранение неполадок.
36. Опишите основные угрозы безопасности, характерные для облачных служб, и их влияние на защиту данных.
37. Дайте понятие модели совместной ответственности в облачных вычислениях и охарактеризуйте её роль в обеспечении безопасности.
38. Перечислите ключевые методы шифрования данных в облачных службах и объясните их значение для предотвращения утечек информации.
39. Охарактеризуйте подходы к управлению доступом и аутентификации пользователей в облачных средах.
40. Раскройте особенности обеспечения соответствия стандартам безопасности и конфиденциальности в облачных службах.
41. Настройте политику контроля учетных записей пользователей (UAC) в Windows 10/11 для повышения уровня безопасности системы.
42. Выполните настройку встроенного брандмауэра Windows 10/11, добавив правило для блокировки или разрешения определённого трафика.
43. Реализуйте настройку шифрования дисков с использованием BitLocker в Windows 10/11 и объясните, как это повышает защиту данных.
44. Создайте и настройте политику групп (Group Policy) для ограничения использования небезопасных приложений в Windows 10/11.
45. Настройте автоматическое обновление системы в Windows 10/11, обеспечив регулярное применение критических обновлений безопасности.
46. Настройте правила доступа в межсетевом экране (firewall) маршрутизатора для ограничения нежелательного входящего и исходящего трафика.
47. Реализуйте конфигурацию безопасного удалённого доступа к сетевому устройству, используя протоколы SSH или VPN.
48. Реализуйте изменение стандартных логинов и паролей на сетевых устройствах для предотвращения несанкционированного доступа.
49. Настройте правила фильтрации URL на сетевом устройстве для ограничения доступа к нежелательным веб-ресурсам.
50. Выполните настройку резервного копирования конфигурации сетевого устройства для обеспечения восстановления системы в случае сбоя.
51. Настройте SSH-доступ в Linux, изменив порт по умолчанию и отключив вход с использованием пароля, используя командную строку.
52. Реализуйте настройку ограничений на выполнение программ с использованием команд chmod и chown для управления правами доступа.
53. Создайте резервную копию системных данных с использованием утилиты rsync и настройте её выполнение по расписанию через cron.
54. Настройте логирование событий системы с помощью syslog или journalctl для отслеживания и анализа попыток несанкционированного доступа.
55. Реализуйте модель машинного обучения для обнаружения вредоносного кода, используя набор данных с характеристиками файлов.
56. Настройте и обучите модель классификации для определения подозрительных сетевых пакетов, используя алгоритм SVM или логистическую регрессию.
57. Разработайте модель на основе нейронных сетей для анализа логов событий системы и выявления аномалий в поведении пользователей.
58. Постройте модель машинного обучения для прогнозирования уязвимостей программного обеспечения на основе его исходного кода.
59. Постройте модель для анализа электронных писем и определения спам-сообщений с помощью методов обработки текста (NLP).
60. Опишите применение моделей машинного обучения для защиты от SQL-инъекций в веб-приложениях