Вопросы для проведения зачёта по дисциплине «Программные средства защиты информации».

1. Методы контроля целостности информации в автоматизированных системах.
2. Методы привязки программного обеспечения к аппаратным частям компьютера.
3. Базовые методы шифрования информации. Понятие симметричной и ассиметричной криптографии.
4. Методы шифрования данных. Симметричная криптография. Алгоритм DES, базовые понятия и режимы работы.
5. Методы обеспечения резервного копирования информации. Организация резервного копирования информации на сменные носители, в защищённую область диска, на виртуальный диск, в скрытое пространство, а так же в облачное хранилище.
6. Методы защиты баз данных. Понятие мандатного доступа.
7. Методы резервного копирования баз данных. Организаций репликации данных. Настройка периодичности копирования. Настройка мандатного доступа и привилегий, необходимых для выполнения процедур.
8. Методика экранирования локальной вычислительной сети. Понятие и виды межсетевых экранов.
9. Понятие систем обнаружения вторжений. Методы подключения, последовательная и параллельная схема.
10. Методика тунелирования локальных вычислительных сетей. Понятие VLAN. Организация VPN соединений. Ассиметричная криптография, базовые сведения. Утилита генерации сертификатов Easy RSA.
11. Методы защиты программного обеспечения от нелегального копирования. Понятие ключа защиты. Временные ключи.
12. Антивирусное программное обеспечение. Сигнатурное и эвристическое сканирование. Антивирусное ПО, рекомендованное ФСТЭК РФ.
13. Методика организации мандатного доступа к рабочему месту пользователя.
14. Программные средства защиты рабочих станций от несанкционированного доступа.

15. Программные средства организации доверенной загрузки рабочих станций.
16. Методы контроля запуска приложений пользователем. Понятие замкнутой программной среды. Основные сведения о ПО Secret Net Studio.
17. Методы организации мандатного доступа к вычислительным ресурсам предприятия при помощи программных средств. Работа с пакетом Dallas Lock.
18. Программное обеспечение, используемое для поддержки расследования инцидентов безопасности. Понятие SIEM систем.
19. Типовые векторы атак на вычислительные системы. Атаки типа маскарад. Атаки типа «Человек посередине». Атаки, направленные на временный вывод из строя инфраструктуры предприятия, путём исчерпания ресурсов канала связи, или DDoS атаки.
20. Основные категории нарушителей в автоматизированных системах обработки информации.
21. Понятие угрозы информационной безопасности. Связь угроз ИБ с уязвимостями программного обеспечения.
22. Атаки направленные на повышение привилегий пользователя.
23. Типовые барьеры обороны, используемые в информационных системах обработки инфомрации.
24. Иные методы защиты информации, не рекомендованные к использованию. Использования приманок с целью контроля работы системы защиты информации.
25. Основные этапы проведения атак на иформационно - измерительные системы.
26. Основные методы сбора информации об объекте защиты.
27. Использование дополнений и специализированных поисковых систем для сбора предварительной информации об объекте защиты, Google dorks, Shodan.io, Censys.io, ViewDNSInfo, 2ip.
28. Методы сбора информации, на основе открытых данных. Osint Framework.
29. Анализ истории действий пользователя, на основе архивной информации, web.archive.org.
30. Методы сканирования объеков защиты на основе специализированных средств. NMap?
31. Назначение и основные функции сканера NMap?
32. Методы сбора конфигурации сети исследуемой системы и поиска данных об установленных приложения и версиях служб.

33. Базовые методы поиска уязвимостей в АС, на основе приложения NMap? Правовые последствия и ограничения?
34. Методы обеспечения анонимности и обхода средств защиты при использовании NMap?
35. Основные типы уязвимостей АС? Понятие эксплойта?
36. Структура и базовые параметры команд Metasploit Framework?
37. Основные типы соединений с исследуемой системой, используемые в Metasploit Framework?
38. Базовая методика применения Metasploit Framework для анализа защиты систем?
39. Понятие полезной загрузки, используемой в Metasploit Framework? Виды полезных нагрузок.
40. Методы доставки эксплойтов на исследуемые системы? Дополнительные средства Metasploit Framework, используемые для данных целей?
41. Методы псевдообращения хеш-функций. Понятие брутинга. Методы брутинга хешей, радужные таблицы?
42. Понятие словарей данных и использование словарей для поиска соответствий? Основные приложения и словари, используемые для автоматизации подобных процедур?
43. Методика применения приложения HashCat?
44. Состав комплекса и методика применения приложения JhonTheRipper?
45. Основные методы хранения паролей в ОС и способы несанкционированного доступа к ним и получения их значений?
46. Методы автоматизации работы с ПК Metasploit Framework, базовые методы построения графического интерфейса, необходимого для работы с данным приложением?
47. Методика работы приложения Armitage. Основные проблемы, возникающие при работе с ним и методика его применения?
48. Базовые методы построения Web приложений? Основные векторы атак на Web приложения?
49. Методы перехвата трафика. Понятие проксирования. Основные прокси серверы, используемые в ОС Linux, для анализа систем защиты?
50. Основные возможности приложений Burp Suite и OWASP ZAP? Типовые методы использования?
51. Виды атак на Web приложения, реализуемые при помощи Burp Suite и OWASP ZAP? Интеграция браузера и прокси сервера.

52. Основные модули платформы DVWA?
53. Понятие и виды SQL инъекций?
54. Методы поиска инъекций в АС?
55. Сравнение платформ DVWA и bwApp, в части методов тестирования SQL инъекций. Основные различия уровней сложности платформ?
56. Методы организации хостинга Web приложений?
57. Методика определения скрытых каталогов Web приложений?
58. Сравнение средств анализа каталогов приложений DirSearch, DirBuster, GoBuster. Понятие словаря поиска.
59. Правовое обеспечения исследования уязвимостей в АС. Статьи УК РФ. Приказы ФСТЭК и постановления правительства РФ. Виды ответственности и условия соблюдения законности данных процедур?