Оценочные материалы для промежуточной аттестации по дисциплине

«Программно-аппаратные средства обеспечения информационной», 8 семестр

Код, направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Безопасность информационных систем и технологий
Форма обучения	очная
Кафедра-разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

Типовые темы контрольной работы

1. Классификация методов и средств программно-аппаратной защиты информации.
2. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно- аппаратными средствами.
3. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
4. Методы создания безопасных систем.
5. Методология проектирования гарантированно защищенных КС.
6. Источники дестабилизирующего воздействия на объекты защиты.
7. Причины и условия дестабилизирующего воздействия на информацию.
8. Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД.
9. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.
10. Особенности защиты данных от изменения. Шифрование.
11. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды.
12. Понятие АМДЗ (доверенная загрузка).
13. Применение закладок, направленных на снижение эффективности средств, замыкающих среду.
14. Задачи защиты ПО от изучения и способы их решения. Защита ПО от дизассемблирования.
15. Вредоносное программное обеспечение как особый вид разрушающих воздействий.
16. Классификация вредоносного программного обеспечения.
17. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.
18. Поиск следов активности вредоносного ПО.

19. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО.
20. Ботнеты. Принцип функционирования. Методы обнаружения.
21. Классификация антивирусных средств. Сигнатурный и эвристический анализ.
22. Защита от вирусов в "ручном режиме".
23. Основные концепции построения систем антивирусной защиты на предприятии.
24. Несанкционированное копирование программ как тип НСД.
25. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.
26. Защитные механизмы в современном программном обеспечении на примере MS Office.
27. Проблема защиты отчуждаемых компонентов ПЭВМ.
28. Методы защиты информации на отчуждаемых носителях. Шифрование.
29. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.
30. Безвозвратное удаление данных. Принципы и алгоритмы.
31. Устройства Touch Memory.
32. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ.
33. Использование сетевых снифферов в качестве СОВ.
34. Аппаратный компонент СОВ. Программный компонент СОВ.
35. Классификация систем обнаружения вторжений.
36. Обнаружение сигнатур.
37. Обнаружение аномалий.
38. Штатные средства защиты информации стека протоколов TCP/IP.
39. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP,
40. достоинства, недостатки, ограничения.
41. Виртуальная частная сеть. Функции, назначение, принцип построения.
42. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.
43. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.
44. Основные типы firewall. Симметричные и несимметричные firewall.
45. Однохостовые и мультихостовые firewall.
46. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту, исходя из архитектуры и выполняемых функций.
47. Основные типы угроз. Модель нарушителя.
48. Средства идентификации и аутентификации. Управление доступом.
49. Средства контроля целостности информации в базах данных.
50. Средства аудита и контроля безопасности. Критерии защищенности баз данных.
51. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.
52. Классификация сетевых мониторов.
53. Системы управления событиями информационной безопасности (SIEM).

Типовые вопросы к экзамену

1. Идентификация субъекта
2. Идентифицирующая информация
3. Понятие защищённой системы
4. Правила разграничения доступа
5. Модели ОС. Сравнительный анализ ОС
6. Избирательное разграничение доступа
7. Изолированная программная среда
8. Полномочное разграничение доступа без контроля информационных потоков
9. Полномочное разграничение доступа
10. Матрица доступа и вектор доступа
11. Обеспечение конфиденциальности (правила NRU и NWD)
12. Критерии информационной безопасности
13. Технология ЭЦП
14. Понятие “лобовой атаки”, методы формирования паролей
15. Методы борьбы с подбором идентифицирующей информации
16. Методы борьбы с подбором паролей, полученных на основе ошибок администратора
17. Методы борьбы с подбором паролей, полученных на основе ошибок реализации
18. Социальная психология и иные способы получения паролей
19. Принципы построения криптосистем
20. Уровни криптосистем
21. Компоненты Криптосистем
22. Функции Криптосистем
23. Методы получения “случайности”
24. Принципы построения генераторов ПСП и ИСП.
25. Архивация. Алгоритмы архивации
26. Генерация ключей. Распределение ключей. Главный ключ.
27. Восстановление системы при компрометации ключей
28. Классификация криптоалгоритмов
29. Симметричные криптоалгоритмы
30. Асимметричные криптоалгоритмы
31. Технология Хэш-функций
32. Криптосистема семейства программ ViPNet.
33. Состав и назначение компонентов ViPNet [Администратор]
34. Состав и назначение компонентов ViPNet [Координатор]
35. Состав и назначение компонентов ViPNet [Клиент]
36. Состав и назначение компонентов ViPNet [Криптомания]
37. Состав и назначение компонентов ViPNet [PersonalFirewoll]
38. Назначение и принципы построения VPN
39. Формирование структуры виртуальной сети ViPNet
40. Формирование ключевой информации ViPNet
41. Содержание ключевого набора и *.dst – файла Формирование ключей при изменениях в структуре своей сети
42. Межсетевое взаимодействие ViPNet
43. Противодействие изучению исходных текстов
44. Противодействие анализу двоичного кода
45. Защита от РПВ
46. Классификация РПВ

47. Методы и средства защиты информации от технических сбоев, поломок, стихийных бедствий
48. Понятие избыточности
49. Принципы функционирования систем в чрезвычайных условиях. Восстановление работоспособности систем