Областное государственное бюджетное образовательное учреждение

среднего профессионального образования

«Смоленский промышленно-экономический колледж»

Контрольно-измерительные материалы комплексного (дифференцированного)

зачета по междисциплинарным курсам

МДК.03.01 Технические методы и средства, технологии защиты информации и МДК.03.02 Программно-аппаратные средства защиты информации

для студентов 4 курса

специальности 090905 Организация и технология защиты информации

Смоленск 2013

Разработчики: ОГБОУ СПО «Смоленский промышленно-экономический колледж»

Преподаватели: Ромашкова И. А.

Методист:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.С. Тригубова

# I. Паспорт комплекта контрольно-измерительных материалов

## 1.1. Область применения

 Контрольно-измерительные материалы предназначены для проверки результатов освоения междисциплинарных курсов МДК.03.01 Технические методы и средства, технологии защиты информации и МДК.03.02 Программно-аппаратные средства защиты информации основной профессиональной образовательной программы (далее ОПОП) по специальности СПО 090905 Организация и технология защиты информации базовой подготовки.

1.2. Освоение умений и усвоение знаний:

|  |  |
| --- | --- |
| **Освоенные умения, усвоенные знания** | **Показатели оценки результата** |
| **1** | **2** |
| Работать с техническими средствами защиты информации | Техничность работы технических средств защиты информации |
| Работать с защищенными автоматизированными системами | Техничность применения программно-аппаратных защиты информации |
| Передавать информацию по защищенным каналам связи | Соблюдение регламента передачи информации по защищенным каналам связи |
| Фиксировать отказы в работе средств вычислительной техники | Результативность в определении отказов в работе средств вычислительной техники |
| Знать виды, источники и носители защищаемой информации | Точность изложения видов, источников и носителей защищаемой информации |
| Знать источники опасных сигналов | Точность изложения источников опасных сигналов |
| Знать структуру, классификацию и основные характеристики технических каналов утечки информации | Точность изложения структуры, классификации и основных характеристик технических каналов утечки информации |
| Знать классификацию технических разведок и методы противодействия им | Точность изложения классификации технических разведок и методов противодействия им |
| Знать методы и средства технической защиты информации | Точность изложения методов и средств технической защиты информации |
| Знать методы скрытия информации | Точность изложения методов скрытия информации |
| Знать программно-аппаратные средства защиты информации | Точность изложения программно-аппаратных средств защиты информации |
| Знать структуру подсистемы безопасности операционных систем и выполняемые ею функции | Точность изложения структуры подсистемы безопасности операционных систем и выполняемых ею функции |
| Знать средства защиты в вычислительных сетях | Точность изложения средств защиты в вычислительных сетях |
| Знать средства обеспечения защиты информации в системах управления базами данных | Точность изложения средств обеспечения защиты информации в системах управления базами данных |
| Знать критерии защищенности компьютерных систем | Точность изложения критериев защищенности компьютерных систем |
| Знать методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов | Точность изложения методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов |

* 1. **Система контроля и оценки освоения программы учебной дисциплины**

Итоговый контроль освоения программ междисциплинарных курсов проводится в форме (дифференцированного) зачета и предусматривает пятибалльную систему оценки. Зачет проводится в пределах учебного времени, отведенного на изучение дисциплины.

Оценка освоения программ междисциплинарных курсов проводится в соответствии с «Положением о текущем контроле и промежуточной аттестации студентов ОГБОУ СПО «Смоленский промышленно-экономический колледж»» и рабочим учебным планом по специальности.

* 1. **Вопросы и практические задания к зачету.**

1. Классификация угроз информационной безопасности.

2. Классификация технических каналов утечки информации.

3. Прямой акустический канал утечки информации.

4. Виброакустический канал утечки информации.

5. Акустоэлектрический канал утечки информации.

6. Акустооптический канал утечки информации.

7. Параметрический (акустический) канал утечки информации.

8. Электромагнитный канал утечки информации.

9. Визуально-оптический и материально-вещественный каналы утечки информации.

10. Утечки информации по цепям заземления и электропитания.

11.Классификация методов защиты информации.

12.Экранирование узлов и соединений аппаратуры. Снижение уровней наводок на проводные тракты и узлы аппаратуры.

13. Пассивные методы защиты речевой информации (звукоизоляция помещений).

14. Активные методы защиты речевой информации (акустическая маскировка).

15.Технические средства обнаружения закладных устройств.

16. Технические средства охраны периметра.

17. Охранное телевидение.

18. Системы контроля и управления доступом.

19. КУИ в АС. Классификация. Уровни взаимодействия АС.

20. Методы и средства защиты информации от НСД.

21. Механизмы защиты информации от НСД.

22. Требования по ЗИ от НСД. Показатели защищенности СВТ по ЗИ от НСД.

23. Общие сведения о системе сертификации средств ЗИ. Порядок проведения сертификации средств ЗИ и защищенных АС и СВТ.

24. Идентификация и аутентификация субъектов и объектов АС. Понятие протокола аутентификации.

25. Подходы к реализации средств аутентификации и идентификации. Средства аутентификации пользователей.

26. Понятие политики безопасности. Принципы реализации

27. Иерархический доступ к файлу. Особенности, связь с достоверной вычислительной базой.

28. Доступ  данным со стороны скрытого процесса. Понятие скрытого доступа.

29. Программные и аппаратные средства разграничения доступа. Надежность систем разграничения доступа.

30. Модель разграничения доступа к информации в АС. Понятие, порядок разработки.

31. Разрушающее программное воздействие. Понятие, причины НСД при использовании ПО.

32. Программные закладки. Понятие, методы внедрения.

33. Контрольно-испытательные методы анализа безопасности ПО.

34. Логико-аналитические методы анализа безопасности ПО.

35. Компьютерные вирусы как особый класс РПВ. Сущность и проявление КВ.

36. Принцип построения и функционирование программных антивирусных средств.

**Практические задания.**

1. Имея права администратора восстановите пароль учетной записи с ограниченными правами сотрудника фирмы и войдите в систему.

2. Настройте адекватную политику безопасности компьютера, удовлетворяющую обеспечению надежной защиты операционной системы.

3. Произведите установку и настройку Персонального Средства Криптографической защиты (далее СКЗИ) «Шипка 1.5» и составьте для персонала инструкцию по его эксплуатации.

4. Произведите установку и настройку оборудования - биометрической флэш – памяти nTegrity Pro Vista и составьте инструкцию по эксплуатации для пользователя.

5. Произведите установку и настройку оборудования - мышь со считывателем отпечатка пальца – EyeD Opti Mouse и составьте инструкцию по эксплуатации для пользователя.

6. Произведите установку и настройку оборудования - комплекс СЗИ НСД «Аккорд - АМДЗ» и составьте инструкцию по эксплуатации для пользователя.

7. Произведите установку и настройку оборудования - АПМДЗ «КРИПТОН - ЗАМОК» и составьте инструкцию по эксплуатации для пользователя.

8. Произведите установку и настройку оборудования - средства аутентификации «Рутокен» и составьте инструкцию по эксплуатации для пользователя.

9. Произведите установку и настройку оборудования - аппаратного комплекса защиты конфиденциальной информации «Aladdin. SecretDisk» и составьте инструкцию по эксплуатации для пользователя.

10. Определите адекватную политику безопасности компьютера и произведите её настройку. На компьютере уже выполнены настройки, не позволяющие открывать консоль mmc даже в режиме Администратора.

* 1. **Литература**
1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2009. – 616 с.
2. Хореев П.Б. Программно-аппаратная защита информации: учебн. пособие для вузов по спец-ти «Информационная безопасность», «Информатика и вычислительная техника» / П.Б. Хореев. – М.: ФОРУМ, 2011. – 351 с.