Министерство образования и науки Республики Дагестан
Государственное бюджетное профессиональное образовательное учреждение
Республики Дагестан
«Кизлярский профессионально-педагогический колледж»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине ОП.02 Организационно - правовое обеспечение информационной безопасности

Код и наименование специальности: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Форма обучения: очная

Кизляр, 2022г.

Фонд оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Разработчики:

__Махтаев Ш.И., преподаватель ГБПОУ РД КППК_____
(место работы) (занимаемая должность) (инициалы, фамилия)

Рассмотрено и одобрено ПЦК _профессиональных дисциплин по техническим специальностям_____

Протокол № 1 от 31 08 2022 г.

Председатель ПЦК ___Раджабова А.Н. /_____
(ФИО) *(подпись)*

1. Общие положения

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, осваивающих программу учебной дисциплины ОП.02 Организационно-правовое обеспечение информационной безопасности.

КОС включают материалы для проведения текущего, рубежного контроля и промежуточной аттестации в форме дифференцированного зачета.

2. Структура контрольных заданий

2.1. Типовые задания для текущего контроля:

Вопросы для устного опроса по теме Сертификация и аттестация по требованиям безопасности информации

1. Организационная структура системы сертификации средств криптографической защиты информации.
2. Назовите виды и схемы сертификации средств криптографической защиты информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств криптографической защиты информации?
4. Особенности порядка подготовки и проведения сертификации средств криптографической защиты информации.
5. Виды контроля в области сертификации средств криптографической защиты информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.
8. Какие средства относятся к шифровальным?
9. Что относится к закрытым телекоммуникационным системам и комплексам?
10. Дайте определение аттестации объектов информатизации по требованиям безопасности информации.
11. Виды аттестации помещений по требованиям безопасности информации.
12. Какие помещения подлежат обязательной аттестации?
13. Порядок проведения аттестации помещений по требованиям безопасности информации.
14. Какая документация представляется органу по аттестации?
15. Содержание заключения аттестационной проверки помещения.
16. Содержание протокола аттестационных испытаний помещения.
17. Содержание аттестата соответствия на объект информатизации.

Практическая работа Подготовка документов к аттестации объектов информатизации
Контрольные вопросы:

1. Организационная структура системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.

2. Назовите виды и схемы сертификации средств вычислительной техники и связи по требованиям безопасности информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств вычислительной техники и связи по требованиям безопасности информации?
4. Особенности порядка подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.
5. Виды контроля в области сертификации средств вычислительной техники и связи по требованиям безопасности информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.
8. Назовите показатели защищенности.
9. Сколько классов защищенности существует?
10. Сформулируйте требования к показателям защищенности.

2.2. Типовые задания для рубежного контроля:

Вопросы для устного опроса по разделу «Организационно - правовое обеспечение информационной безопасности»

1. Охарактеризуйте информацию и ее основные показатели.
2. Какие существуют подходы к определению понятия «информация».
3. В чем заключается двуединство документированной информации с правовой точки зрения.
4. Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.
5. К какому виду информации относится записанный на бумаге текст программы для ЭВМ?
6. Назовите основные виды конфиденциальной информации.
7. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
8. Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?
9. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
10. Назовите основные цели государства в области обеспечения информационной безопасности.
11. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
12. Какой закон определяет понятие «официальный документ»?
13. Какой закон определяет понятие «электронный документ»?
14. В тексте какого закона приведена классификация средств защиты информации?
15. Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?
16. Назовите основные положения Доктрины информационной безопасности РФ.
17. Назовите составляющие правового института государственной тайны.
18. В каких случаях нельзя относить информацию к государственной тайне?

19. Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?
20. Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.
21. Дайте определение системы защиты государственной тайны и укажите ее составляющие.
22. Что в соответствии с законодательством РФ представляет собой засекречивание информации.
23. Перечислите основные принципы засекречивания информации.
24. Что понимается под профессиональной тайной?
25. Какие виды профессиональных тайн вам известны?
26. В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?
27. В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?
28. Что представляет собой электронная цифровая подпись?
29. Каковы основные особенности правового режима электронного документа?
30. Назовите основные ограничения на использование электронных документов?

Вопросы для устного опроса по разделу «Лицензирование и сертификация в области защиты информации»

1. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
2. Организационная структура системы государственного лицензирования в области защиты информации.
3. Функции государственных органов по лицензированию в области защиты информации.
4. Функции лицензионных центров по лицензированию в области защиты информации.
5. Права и обязанности лицензиатов.
6. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
7. Назовите случаи приостановления или прекращения действия лицензии.
8. В каких случаях предприятию отказывают в выдаче лицензии?
9. Какие документы предоставляются для получения лицензии?
10. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
11. Какие средства относятся к шифровальным?
12. Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
13. Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.
14. Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

15. Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.
16. Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

2.3. Типовые задания для промежуточного контроля:

Вопросы для подготовки к дифференцированному зачету

1. Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС.
2. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.
3. Основные особенности современных проектов АИС. Электронный документооборот.
4. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные.
5. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение.
6. Модели жизненного цикла АИС.
7. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.
8. Требования к автоматизированной системе в защищенном исполнении.
9. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении.
10. Требования по защите сведений о создаваемой автоматизированной системе.
11. Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации.
12. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации
13. Понятие уязвимости угрозы. Классификация уязвимостей.
14. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.
15. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним
16. Идентификация и аутентификация субъектов доступа и объектов доступа.
17. Управление доступом субъектов доступа к объектам доступа.

18. Ограничение программной среды.
19. Защита машинных носителей информации
20. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения.
21. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.
22. Обнаружение (предотвращение) вторжений
23. Контроль (анализ) защищенности информации
24. Обеспечение целостности информационной системы и информации
25. Обеспечение доступности информации
26. Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.
27. Защита технических средств.
28. Защита информационной системы, ее средств, систем связи и передачи данных
29. Резервное копирование и восстановление данных.
30. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.
31. Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.
32. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.
33. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.
34. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.
35. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении
36. Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью.
37. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями.
38. Управление, тестирование и эксплуатация автоматизированных систем.
39. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
40. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.
41. Общие обязанности администратора информационной безопасности автоматизированных систем.
42. Основные принципы защиты от НСД. Основные способы НСД.

43. Основные направления обеспечения защиты от НСД. Организация работ по защите от НСД.
44. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.
45. Классификация автоматизированных систем. Требования по защите информации от НСД для АС
46. Требования защищенности СВТ от НСД к информации
47. Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ
48. Модели управления доступом.
49. Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами.
50. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.
51. Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий.
52. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.
53. Обеспечение целостности информационной системы и информации
54. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности
55. Механизмы защиты информации.
56. Технологии безопасности беспроводных сетей и унифицированные решения.
57. Протоколы и функции, применяемые в межсетевых экранах и интернет-маршрутизаторах.
58. Протоколы IGMP и UPnP. Качество обслуживания и Технология SharePort.
59. Фильтрация трафика и виртуальные сети.
60. Технология преобразования сетевых адресов, механизмы PAT и NAT.
61. Функции IDP, WCF, AV и технология ZoneDefense.
62. Особенности применения межсетевых экранов и маршрутизаторов D-Link.
63. Управление межсетевыми экранами D-Link NetDefend.
64. Основные эксплуатационные документы защищенных автоматизированных систем.
65. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем.
66. Акт ввода в эксплуатацию на автоматизированную систему.
67. Технический паспорт на защищаемую автоматизированную систему.
68. Основные сертифицированные программно-аппаратные средства по защите информации, их назначение, функции, настройка, применение.