

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**по учебной дисциплине ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

Код и наименование специальности (профессии): 10.05.02 Обеспечение
информационной безопасности автоматизированных систем

Форма обучения

Кизляр, 2023 г.

Фонд оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности/профессии СПО (10.05.02 Обеспечение информационной безопасности автоматизированных систем)

Разработчики:

Заманов Б.Х., преподаватель ГБПОУ РД КППК

(место работы) (занимаемая должность) (инициалы, фамилия)

Рассмотрено и одобрено ПЦК профессиональных дисциплин по
техническим специальностям

Протокол № 1 от 29 08 2023 г.

Председатель ПЦК Раджабова А.Н. / А. Н.
(ФИО) (подпись)

СОДЕРЖАНИЕ

1. Общие положения	4
2. Структура контрольных заданий	5
2.1.Задания текущего контроля	5
2.2.Задания рубежного контроля	6
2.3.Задания для промежуточной аттестации	7

1. Общие положения

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, осваивающих программу учебной дисциплины ОП.01 Основы информационной безопасности.

КОС включают контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме экзамена:

Наименование результата обучения

Результаты обучения (освоенные умения, усвоенные знания)

Код ПК, ОК	Умения	Знания
ОК 03, ОК 06, ОК 09,	<ul style="list-style-type: none"> – классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации; 	<ul style="list-style-type: none"> – сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; – источники угроз безопасности информации и меры по их предотвращению; – факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности; – основные методики анализа угроз и рисков информационной безопасности;

2. Структура контрольных заданий

2.1.Задания текущего контроля

Тема 1.1 Основные понятия и задачи информационной безопасности

Задание для устного опроса по темам

1. Понятия информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Обзор защищаемых объектов и систем.
4. Понятие «угроза информации».
5. Понятие «риск информационной безопасности».
6. Примеры преступлений в сфере информации и информационных технологий.
7. Сущность функционирования системы защиты информации.
8. Защита человека от опасной информации и от неинформированности в области информационной безопасности

Тема 1.2 Нормативно правовое регулирование защиты информации

Задание для устного опроса по темам

1. Организационная структура системы защиты информации. 2. Законодательные акты в области защиты информации.
3. Российские и международные стандарты, определяющие требования к защите информации.
4. Система сертификации РФ в области защиты информации.
5. Основные правила и документы системы сертификации РФ в области защиты информации

Тема 1.3 Классификация безопасности

Задание для устного опроса по темам

1. Целостность, доступность и конфиденциальность информации.
2. Классификация информации по видам тайны и степеням конфиденциальности.
3. Понятия государственной тайны и конфиденциальной информации.
4. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
5. Цели и задачи защиты информации.
6. Основные понятия в области защиты информации
7. Элементы процесса менеджмента ИБ.
8. Модель интеграции информационной безопасности в основную деятельность организации.
9. Понятие политики безопасности

Тема 2.1 Угрозы безопасности защиты информации и основы защиты информации

Задание для устного опроса по темам

1. Понятие угрозы безопасности информации.
2. Системная классификация угроз безопасности информации.

3. Каналы и методы несанкционированного доступа к информации.
4. Уязвимости. Методы оценки уязвимости информации.

Тема 2.2 Методологические подходы к защите информации

Задание для устного опроса по темам

1. Анализ существующих методик определения требований к защите информации.
2. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
3. Виды мер и основные принципы защиты информации

Критерии оценки

«Отлично» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;
- доказательно раскрыты основные понятия, термины и др.;
- в ответе отслеживается четкая структура, выстроенная в логической последовательности;
- ответ изложен грамотным языком;
- на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

«Хорошо» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные моменты материала;
- ответ четко структурирован, выстроен в логической последовательности; - изложен грамотным языком;
- однако были допущены неточности в определении понятий, терминов и др.

«Удовлетворительно» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют некоторые нарушения;
- допущены несущественные ошибки в изложении теоретического материала и употреблении терминов;
- знания показаны слабо, речь неграмотная.

«Неудовлетворительно» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения;
- допущены существенные ошибки в теоретическом материале (понятиях, терминах); - знания отсутствуют, речь неграмотная.

2.2.Задания рубежного контроля

Контрольная работа № 1 «Теоретические основы информационной безопасности».

Цель: проверить теоретические знания и практические навыки по темам дисциплины ОП.01 «Основы информационной безопасности».

Задание. Ответить на поставленные вопросы

Вариант 1

1. Понятие «угроза информации».

2. Классификация информации по видам тайны и степеням конфиденциальности.
3. Понятия государственной тайны и конфиденциальной информации.
4. Каналы и методы несанкционированного доступа к информации.

Вариант 2

1. Понятие «риска информационной безопасности».
2. Системная классификация угроз безопасности информации.
3. Понятие политики безопасности.
4. Уязвимости. Методы оценки уязвимости информации

Критерии оценки

Отметкой «отлично» оцениваются ответы, которые показывают прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, давать аргументированные ответы, приводить примеры.

Отметкой «хорошо» оцениваются ответы, обнаруживающие прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, приводить примеры. Однако допускаются две-три неточности в ответах.

Отметкой «удовлетворительно» оцениваются ответы, свидетельствующие в основном о знании материалов, их свойств, технологий, но отличающиеся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа тем изучаемой дисциплины, недостаточным умением давать аргументированные ответы и приводить примеры. Допускается несколько ошибок в содержании ответа.

Отметкой «неудовлетворительно» оцениваются ответы, обнаруживающие незнание материалов, их свойств, технологий изучаемой предметной области, отличающиеся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа тем изучаемой дисциплины; неумением давать аргументированные ответы. Допускаются серьезные ошибки в содержании ответов.

2.3.Задания для промежуточной аттестации

Экзамен проводится по учебной дисциплине в устной форме по вопросам, в которых отражена проверка освоения обучающимися умений и знаний.

Критерии оценки:

Оценка освоения осуществляется по результатам ответа экзаменуемого.

Оценка «отлично» – выставляется при полном самостоятельном ответе на предложенные вопросы: теоретический материал раскрыт полностью, обучающийся владеет знаниями и умениями, может объяснить их применение на практике.

Оценка «хорошо» – выставляется при полном ответе на предложенные вопросы: теоретический материал раскрыт полностью, обучающийся владеет знаниями теории,

может объяснить их применение на практике, но в ответе есть неточности, допущена нарушение логики вопроса.

Оценка «удовлетворительно» – обучающийся владеет знаниями и умениями, может объяснить их применение на практике, но в ответе есть неточности, не достаточно раскрыты ответы на поставленные вопросы, ответ не самостоятельный, допущены ошибки при формулировании основных позиций теории и применения их на практике.

Оценка «неудовлетворительно» – обучающийся недостаточно владеет знаниями и умениями, допускает грубые ошибки и неточности во время ответа, ответ на поставленные вопросы не дан.

Вопросы к экзамену по учебной дисциплине « Основы информационной безопасности»

1. Дайте характеристику составляющих "информационной безопасности" применительно к вычислительным сетям.
2. Перечислите основные механизмы безопасности.
3. Какие механизмы безопасности используются для обеспечения конфиденциальности трафика?
4. Какие механизмы безопасности используются для обеспечения "неотказуемости" системы?
5. Что понимается под администрированием средств безопасности?
6. Какие виды избыточности могут использоваться в вычислительных сетях?
7. Как обнаружить загрузочный вирус?
8. Характерные черты макровируса.
9. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?
10. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
11. Особенности заражения компьютеров локальных сетей.
12. Как ограничить заражение макровирусом при работе с офисными приложениями?
13. Как обнаружить резидентный вирус?
14. Как проверить систему на наличие макровируса?
15. Перечислите основные этапы алгоритма обнаружения вируса.
16. Какие особенности заражения вирусами при использовании электронной почты?
17. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
18. Как ограничить заражение макровирусом при работе с офисными приложениями?
19. Как рассматривается сеть в концепции протокола IP?
20. Преобразуйте IP-адрес "11110011 10100101 00001110 11000001" в десятичную форму.
21. Из каких частей состоит IP-адрес?
22. Для чего предназначен DNS-сервер?
23. Перечислите классы удаленных угроз.
24. Как классифицируются удаленные угрозы "по характеру воздействия"?
25. Охарактеризуйте удаленные угрозы "по цели воздействия".
26. Дайте определение маршрутизатора.
27. Что такое подсеть и сегмент сети? Чем они отличаются?
28. Что такое IP-адрес?
29. Сколько классов сетей определяет IP протокол?
30. К какому классу относится следующий адрес: 199.226.33.168?

31. Какой из этих адресов не может существовать: 109.256.33.18 или 111.223.44.1?
32. Поясните понятие домена.
33. В чем заключается иерархический принцип системы доменных имен?
34. Как классифицируются удаленные угрозы "по расположению субъекта и объекта угрозы"?
35. Может ли пассивная угроза привести к нарушению целостности информации?
36. Что такое подсеть и сегмент сети? Чем они отличаются?
37. Перечислите основные причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях.
38. Почему виртуальное соединение не обеспечивает требуемого уровня защиты вычислительных сетей?
39. Какая из причин приводит к успеху удаленной угрозы "анализ сетевого трафика"?
40. В чем заключаются преимущества сети с выделенными каналами?
41. Какие алгоритмы удаленного поиска Вам известны?
42. Какой из алгоритмов поиска более безопасный?
43. Что является следствием недостаточной аутентификации субъектов и объектов вычислительных сетей?
44. К чему приводит недостаточность информации об объектах вычислительной сети? Приведите пример.
45. Может ли быть нарушена целостность информации при отсутствии в распределенных вычислительных сетях возможности контроля за маршрутом сообщений? Почему?
46. Как повысить защищенность вычислительных сетей при установлении виртуального соединения?
47. Как можно защитить сеть от реализации атаки "отказ в обслуживании"?
48. Как можно контролировать маршрут сообщения в сети?
49. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
50. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
51. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
52. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
53. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
54. Понятие политики безопасности информационных систем. Назначение политики безопасности.
55. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
56. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
57. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
58. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
59. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.

60. Основные положения руководящих документов Гостехкомиссии России.
Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
61. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
62. Единые критерии безопасности информационных технологий. Проект защиты.
Требования безопасности (функциональные требования и требования адекватности).
63. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
64. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
65. Идентификация и аутентификация при входе в информационную систему.
Использование парольных схем. Недостатки парольных схем.
66. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
67. Биометрические средства идентификации и аутентификации пользователей.
68. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
69. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
70. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
71. Законодательный уровень применения цифровой подписи.
72. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
73. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
74. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
75. Средства обеспечения информационной безопасности в ОС Windows. Разграничение доступа к данным. Групповая политика.
76. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
77. Применение средств Windows для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
78. Разграничение доступа к данным в ОС семейства UNIX.
79. Пользователи и группы в ОС UNIX.
80. Пользователи и группы в ОС Windows.
81. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
82. Причины нарушения безопасности информации при ее обработке криптографическими средствами.

83. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
84. Распределенные информационные системы. Удаленные атаки на информационную систему.
85. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
86. Физические средства обеспечения информационной безопасности.
87. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
88. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
89. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
90. Виртуальные частные сети, их функции и назначение.