ПРИЛОЖЕНИЕ №1
к рабочей программе дисциплины
Б1.В.04 «Объекты защиты информации»

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Факультет вычислительной техники

Кафедра «Информационной безопасности»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.В.04 «Объекты защиты информации»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация № 8 «Разработка автоматизированных систем в защищенном исполнении»

ОПОП по специальности

10.05.03 Информационная безопасность автоматизированных систем

Квалификация выпускника – специалитет по защите информации

Форма обучения – очная

Срок обучения – 5,5 лет

Рязань 2022 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной профессиональной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций, обучающихся целям и требованиям основной профессиональной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности универсальных общепрофессиональных и профессиональных компетенций, приобретаемых обучающимися в соответствии с этими требованиями.

Контроль знаний проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков, приобретенных обучающимися в ходе выполнения индивидуальных заданий на практических занятиях. При оценивании результатов освоения практических занятий применяется шкала «зачтено – не зачтено». Количество практических работ и их тематика определена программой дисциплины.

Промежуточный контроль по дисциплине осуществляется проведением экзамена.

2. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

№ п/п	Контролируемые разделы дисциплины	Код контролируемого индикатора достижения компетенции	Вид, метод, форма оценочного мероприятия
1	Введение в дисциплину	ПК-1.1	Экзамен
2	Защита информации как деятельность	ПК-1.1 ПК-1.2 ПК-2.1	Экзамен
3	Носитель информации как объект защиты информации	ПК-1.1 ПК-1.2 ПК-2.1	Экзамен
4	Информационный процесс как объект защиты информации	ПК-1.1 ПК-1.2 ПК-2.1	Экзамен
5	Автоматизированная система как объект защиты информации	ПК-1.1 ПК-1.2 ПК-2.1	Экзамен
6	Объект информатизации как объект защиты информации	ПК-1.1 ПК-1.2 ПК-2.1	Экзамен
7	Условия, в которых осуществляется защита информации	ПК-1.1 ПК-1.2 ПК-2.1	Экзамен

3. ПОКАЗАТЕЛИ И КРИТЕРИИ ОБОБЩЕННЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Результаты обучения по дисциплине	Показатели оценки результата	Критерии оценки результата
ПК – 1.1	Выполняет задания на знание компонентов средств и систем информатизации в защищенном исполнении и свойств вредоносных воздействий на них	Обучающийся должен продемонстрировать знание направлений защиты информации в компьютерных системах, свойств вредоносных воздействий, на противодействие которым эти направления ориентированы, свойства направлений защиты информации. Обучающийся должен продемонстрировать умение определять свойства вредоносных воздействий и необходимые для противодействия им направления защиты информации. Обучающийся должен продемонстрировать владение навыками работы с литературой и ГОСТами в области компьютерной безопасности
ПК – 1.2	Выполнение заданий на применение компонентов систем защиты информации и реализуемых этими компонентами функций по защите информации	Обучающийся должен продемонстрировать знание объектов защиты информации и условий их функционирования, требований о защите информации на объектах информатизации. Обучающийся должен продемонстрировать умение определять необходимые виды и направления защиты информации на объектах информатизации. Обучающийся должен продемонстрировать владение навыками работы с нормативными правовыми актами и методическими документами в области защиты информации
ПК – 2.1	Выполнение заданий на применение знаний и умений определять компоненты объектов защиты информации, требующие контрольные проверки	Обучающийся должен продемонстрировать знание структур, состава и функций комплексных объектов защиты информации и их систем защиты информации. Обучающийся должен продемонстрировать умение определять факторы, воздействующие на защищаемую информацию в комплексных объектах защиты информации. Обучающийся должен продемонстрировать владение навыками работы с инструкциями на средства защиты информации

4. ШКАЛА ОЦЕНКИ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ

В процессе оценки сформированных знаний, умений и навыков обучающегося по дисциплине, производимой на этапе промежуточной аттестации в форме экзамена, используется пятибалльная оценочная шкала:

«Отлично» заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программы. Как правило, оценка «отлично» выставляется обучающимся, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческими способности в понимании, изложении и использовании учебно-программного материала.

«Хорошо» заслуживает обучающийся, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется обучающимся, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

«Удовлетворительно» заслуживает обучающийся, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справляющийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой. Как правило, оценка «удовлетворительно» выставляется обучающимся, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.

«Неудовлетворительно» выставляется обучающемуся, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой знаний. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных знаний по соответствующей дисциплине.

5. ТИПОВЫЕ КОНТРОЛЬНЫЕ ВОПРОСЫ, ЗАДАНИЯ И ИНЫЕ МАТЕРИАЛЫ К ЭКЗАМЕНУ ПО ДИСЦИПЛИНЕ

1. Дайте определение понятия «защита информации».
2. Что такое безопасность информации?
3. Перечислите интегральные характеристики безопасности и дайте им определения.
4. Что такое уязвимость информации, в каких формах она может проявляться?
5. Что относится к составляющим защиты информации как деятельности? Какова их взаимосвязь?
6. Что такое несанкционированное воздействие на защищаемую информацию?
7. Дайте определение термина «отказ».
8. Какое состояние объекта называется работоспособным?
9. Дайте определения видов защиты информации в зависимости от используемых методов и средств защиты информации.
10. Каким образом и с помощью каких средств обеспечивается физическая защита информации?
11. Каким образом и с помощью каких средств обеспечивается техническая защита информации?
12. Что такое средство контроля эффективности защиты информации?

13. Дайте определения понятий:
    а) контроль и управление доступом;
    б) средства контроля и управления доступом;
    в) система контроля и управления доступом;
    г) зона доступа;
    д) точка доступа;
    е) устройство преграждаемое управляемое.
14. Какова общая цель защиты информации?
15. В чем заключается существенное отличие общедоступной информации и информации ограниченного доступа?
16. Каким образом осуществляется определение частных целей защиты информации?
17. В чем заключается деятельность по защите информации от утечки?
18. Чем отличается защита информации от непреднамеренного воздействия от защиты информации от несанкционированного воздействия?
19. Какими способами может осуществляться несанкционированное доведение защищаемой информации до заинтересованных субъектов? Какими свойствами обладает данное вредоносное воздействие?
20. Какими способами может осуществляться получение защищаемой информации агентурными разведками? Какими свойствами обладает данное вредоносное воздействие?
21. Какими способами может осуществляться несанкционированное воздействие на защищаемую информацию без использования специальных средств? Какими свойствами обладает данное вредоносное воздействие
22. Какими способами может осуществляться несанкционированное воздействие на носитель защищаемой информации? Какими свойствами обладает данное вредоносное воздействие?
23. Перечислите и дайте определения составляющих деятельности по защите информации от непреднамеренного воздействия.
24. Каким образом может осуществляться воздействие на защищаемую информацию сбоев и отказов носителей, технических и программных средств обработки защищаемой информации, средств обеспечени ?
25. Какими свойствами обладает данное вредоносное воздействие?
26. Дайте определение понятия «объект защиты информации».
27. На какие классы разделяются объекты защиты информации?
28. Что относится к специальным объектам защиты информации?
29. . По каким причинам затруднительно однозначно определить понятие «информация»?
30. Какие подходы к определению сущности, понятия и свойств информации существуют в настоящее время? Как определяет информацию каждый из них?
31. Какими способами сообщения передаются от источника к их получателю?
32. Какими особенностями обладает информация как объект защиты?
33. Дайте определение элементарного носителя информации.
34. В чем принципиальное отличие элементарного носителя информации от конструктивно законченного носителя информации?
35. Приведите примеры конструктивно законченных носителей информации.
36. Что такое нештатный носитель информации? Приведите примеры таких носителей информации.
37. Сколько свойств штатных и нештатных носителей обрабатываемой информации необходимо учитывать при организации защиты этой информации?
38. Какие свойства нештатных носителей обрабатываемой информации необходимо учитывать при организации ее защиты?

39. Приведите примеры, иллюстрирующие свойства нештатных носителей информации при организации защиты обрабатываемой информации.

40. В чем сущность понятия «информационный процесс»?

41. Что такое техническое задание на создание информационной системы?

42. Чем определяется цель (цели) обработки информации в объекте информационной инфраструктуры?

43. Каким образом и в каком документе задают цели обработки информации в объекте информационной инфраструктуры?

44. На основании чего определяют методы и способы обработки информации?

45. Что такое средства обеспечения объекта информационной инфраструктуры? Приведите примеры таких средств.

46. Какому понятию (составляющей защиты информации как деятельности) эквивалентно понятие «условия, в которых осуществляется обработка информации в информационной системе»?

47. Дайте определение понятия «информационная технология».

48. Какова взаимосвязь между информационной технологией и информационным процессом?

49. По каким признакам классифицируются информационные технологии?

50. Какие системы являются в настоящее время основным видом информационных систем?

51. К какому виду систем относится автоматизированная система ?

52. Дайте определение понятия «задача автоматизированной системы».

53. На какие классы разделяются функции АС по этим классификационным признакам?

54. Дайте определение функций АС, разделяемых по второму классификационному признаку.

55. Что такое интегрированная функция автоматизированной системы ?

56. Какие функции, кроме функций по обработке информации, выполняет автоматизированная система в защищённом исполнении? Дайте определение этим функциям.

57. Назовите основные функции, которые осуществляют специалисты по обеспечению безопасности информации АСЗИ.

58. Почему условия создания (развития) и эксплуатации объекта информационной инфраструктуры являются составляющими этих видов деятельности?

59. Дайте определение понятия «жизненный цикл объекта информационной инфраструктуры».

60. Свойствами и состоянием чего, кого определяются условия создания (развития) и эксплуатации ОИИ?

61. Дайте определение понятия «объект окружающей среды».

62. Как называются явления, действия, процессы, способные оказывать воздействия на защищаемую информацию при эксплуатации или создании ОИИ?

63. По каким признакам целесообразно классифицировать факторы?

64. Дайте определение понятия «внутренний фактор».

65. Приведите примеры:

а) объективных внутренних факторов;

б) объективных внешних факторов;

в) субъективных внутренних факторов;

г) субъективных внешних факторов.

66. В чем некорректность общего определения понятия «угроза безопасности информации»?

67. Что такое не вредоносный фактор?

68. В чем сущность понятия «вредоносное воздействие на объект информационной инфраструктуры»?

69. Дайте определение понятия «штатное воздействие на объект информационной инфраструктуры».

70. Что такое вредоносная составляющая результата вредоносного воздействия на объект информационной инфраструктуры?

71. Какими характерными особенностями может обладать вредоносная составляющая результата нештатного воздействия на объект информационной инфраструктуры?

72. Какие воздействия на объект информационной инфраструктуры можно рассматривать как вредоносные воздействия?

73. Какие нештатные воздействия следует относить к вредоносным воздействиям?

74. Дайте определение понятия «вредоносное воздействие на объект информационной инфраструктуры».

75. Дайте определение понятия «участник вредоносного воздействия».

76. На какие два класса разделяются субъективные вредоносные воздействия? Дайте определение этих классов вредоносных воздействий.

77. Что такое зона оказания вредоносного воздействия?

78. Совокупностями свойств каких двух сущностей определяется опасность реализации вредоносного воздействия?

79. Что является реализацией угроз безопасности информации?

80. Дайте определение понятия «нарушитель безопасности информации».

81. Дайте определение понятия «непреднамеренный нарушитель безопасности информации».

82. По каким признакам классифицируются нарушители безопасности информации?

83. Дайте определение понятия «внутренний нарушитель безопасности информации».

84. Дайте определение всех категорий внутренних нарушителей безопасности информации.

85. Кто может быть внешним злоумышленником?

86. По какому признаку можно разделить лиц, которые могут быть внешними злоумышленниками при эксплуатации ОИИ?

87. Какие возможности наиболее часто использует внешний злоумышленник при создании ОИИ?

88. Какими возможностями обладают внешние непреднамеренные нарушители безопасности информации?

89. Дайте характеристику персоналу ОИИ как нарушителю безопасности информации.

90. По каким признакам и на какие группы разделяются работники оператора ОИИ и уполномоченного лица?

91. Какие работники оператора ОИИ или уполномоченного лица (кроме эксплуатационного персонала ОИИ) могут быть внутренними нарушителями безопасности информации при эксплуатации ОИИ?

92. Как классифицируются внутренние нарушители безопасности информации по уровням возможности и к какой категории внутренних нарушителей безопасности информации они относятся?

93. Какая категория персонала ОИИ может нанести максимальный ущерб пользователю, обладателю защищаемой информации, оператору ОИИ или уполномоченному лицу? Какие предположения о квалификации этой категории персонала ОИИ обычно принимаются?

94. К каким категориям нарушителей относится АХР и каковы его возможности?

95. Дайте определение понятия «модель нарушителя безопасности информации».

96. Назовите примеры задач, для решения которых используют модели нарушителей безопасности информации.

Разработал:
заведующий кафедрой «Информационная безопасность» В.Н. Пржегорлинский

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО ЗАВЕДУЮЩИМ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**08.08.24** 05:26 (MSK)	Простая подпись
ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**08.08.24** 05:26 (MSK)	Простая подпись