Приложение №1

к рабочей программе

дисциплины Б1.В.09

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 «Информационная безопасность»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Б1.В.09 «Методы и средства обнаружения вторжений в автоматизированные системы»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация № 8 «Разработка автоматизированных систем в защищенном исполнении»

Квалификация выпускника: специалист по защите информации

Форма обучения: очная

Срок обучения: 5,5 лет

Рязань, 2023

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 ОПОП.

Основная задача – обеспечить оценку уровня сформированности общекультурных, общепрофессиональных и профессиональных компетенций.

Контроль знаний обучающихся проводится в форме промежуточной аттестации.

Промежуточная аттестация по дисциплине осуществляется проведением экзамена.

2. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или её части)	Наименование оценочного мероприятия
1	2	3	4
1	Тема 1. Введение в дисциплину	ПК-4 ПК-5	Экзамен
2	Тема 2. Основы компьютерных сетей	ПК-4 ПК-5	Экзамен
3	Тема 3. Мониторинг событий информационной безопасности	ПК-4 ПК-5	Экзамен
4	Тема 4. Технические средства обнаружения вторжений	ПК-4 ПК-5	Экзамен
5	Тема 5. Стадия атаки «Разведка»	ПК-4 ПК-5	Экзамен
6	Тема 6. Стадия атаки «Доставка»	ПК-4 ПК-5	Экзамен
7	Тема 7. Стадия атаки «Эксплуатация»	ПК-4 ПК-5	Экзамен
8	Тема 8. Методы автоматизации выявления инцидентов ИБ	ПК-4 ПК-5	Экзамен
9	Тема 9. Стадии атаки «Заражение, Закрепление, Уничтожение следов»	ПК-4 ПК-5	Экзамен
10	Тема 10. Техники кражи учетных данных пользователей в ОС Windows	ПК-4 ПК-5	Экзамен

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

3) эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

Уровень освоения компетенций, формируемых дисциплиной:

Описание критериев и шкалы оценивания теоретического вопроса:

Шкала оценивания	**Критерий**
3 балла (эталонный уровень)	выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя.
2 балла (продвинутый уровень)	выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов.
1 балл (пороговый уровень)	выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя.
0 баллов	выставляется студенту, который не смог ответить на вопрос

На экзамен выносится четыре теоретических вопроса. Максимально студент может набрать 12 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно». Шкала перевода баллов в оценки:

от 10 до 12 баллов - «отлично»;

от 7 до 9 баллов - «хорошо»;

от 3 до 6 баллов - «удовлетворительно»;

менее 3 баллов - «неудовлетворительно»

4. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

Типовые теоретические вопросы:

1. Что такое компьютерная сеть? Чем отличается LAN от WAN?
2. Дайте определение сети Интернет. Является ли сеть Интернет LAN или WAN.
3. Чем модель OSI отличается от модели TCP/IP?
4. Физический уровень модели OSI. Как принято называть данные на данном уровне?
5. Канальный уровень модели OSI. Как принято называть данные на данном уровне?
6. Сетевой уровень модели OSI. Как принято называть данные на данном уровне?
7. Транспортный уровень модели OSI. Как принято называть данные на данном уровне?
8. Сеансовый уровень модели OSI. Как принято называть данные на данном уровне?
9. Уровень представления модели OSI. Как принято называть данные на данном

уровне?

10. Прикладной уровень модели OSI. Как принято называть данные на данном уровне?
11. Что такое инкапсуляция?
12. Что такое порт? На каком уровне OSI используется и для чего.
13. Протокол HTTP. Чем URL отличается от URI? Чем HTTP отличается от HTTPS.
14. Протокол DNS. В чем заключается иерархичность работы данной службы?
15. Протокол DHCP. Что такое время аренды?
16. Протокол POP3. Какие порты по умолчанию использует POP3 и POP3S?
17. Протокол IMAP. Какой порт используется по умолчанию?
18. Протокол SMTP. Какой порт используется по умолчанию?
19. Протокол SSH. Какой порт используется по умолчанию?
20. Протокол FTP. Какой порт используется по умолчанию?
21. Протокол IP. На каком уровне OSI работает? Какие версии существуют и чем отличаются?
22. Протокол UDP. На каком уровне OSI работает? Чем отличается от TCP?
23. Протокол TCP. На каком уровне OSI работает? Чем отличается от UDP?
24. Что такое сетевой концентратор? На каком уровне OSI работает?
25. Что такое сетевой коммутатор? На каком уровне OSI работает?
26. Что такое сетевой маршрутизатор? На каком уровне OSI работает?
27. Что такое VLAN?
28. Что такое VPN?
29. Чем VLAN отличается от VPN?
30. Как работает протокол ARP?
31. Что такое MAC адрес?
32. Что такое IP адрес?
33. NAT. Для чего нужна данная технология и как работает?
34. Дайте определение следующим понятиям: «Защита информации», «Системы защиты информации»
35. Системы класса HIDS. Основные функции и назначение системы.
36. Системы класса NIDS. Основные функции и назначение системы. Чем IPS отличается от IDS?
37. Системы класса Antivirus. Основные функции и способы выявления ВПО.
38. Системы класса DLP. Основные уровни контроля и методы анализа данных.
39. Системы класса WAF. Примеры видов угроз, от которых может защитить WAF.
40. Системы класса Proxy. Виды серверов Proxy. Как используются для защиты информации?
41. Системы класса Firewall. Принципы ограничения доступа к ресурсам.
42. Системы класса Vulnerability Scanner. Основные задачи и методы сканирования.
43. Системы класса Sandbox. Как данные системы можно использовать для защиты информации?
44. Системы класса SIEM.
45. Что такое Cyber-Kill Chain. Как используется для выявления инцидентов ИБ?
46. Дайте определение понятию «Инцидент ИБ». Для чего необходимо проводить расследование инцидентов ИБ?
47. Nmap. На каких стадиях атаки может использоваться? Основные возможности инструмента.
48. Enumeration techniques. На каких стадиях атаки может использоваться? Какую информацию может получить злоумышленник и для чего?
49. Brute-force. На каких стадиях атаки может использоваться? По каким протоколам может осуществляться атака и почему?

50. Какими каналами злоумышленник может осуществить доставку ВПО внутрь защищаемого периметра? Как при этом может быть использована социальная инженерия?
51. Что такое эксплуатация уязвимостей? Какие бывают эксплойты?
52. Что такое Payload и чем он отличается от эксплойта?
53. По каким признакам можно выявить ВПО на защищаемом хосте? Какие СЗИ для этого можно использовать?
54. Как для выявления инцидентов ИБ можно использовать репутацию внешних ресурсов сети Интернет? Что такое C&C?
55. Что такое повышение привилегий? Для каких стадий характерны подобные атаки?
56. Что такое Persistence? Для каких стадий характерны подобные атаки?
57. Опишите пример способа повышения привилегий.
58. Что такое «миграция», для чего используется злоумышленниками?
59. Что такое Pivoting, для чего используется злоумышленниками?
60. Опишите тактики злоумышленника, используемые для уничтожения следов.
61. Что такое SAM в ОС Windows? Какие атаки на SAM могут использоваться злоумышленниками и зачем.
62. За что отвечает служба LSASS в ОС Windows. Какие существуют риски ИБ? связанные с этой службой?
63. Что такое NTDS.DIT? Какие атаки могут использоваться злоумышленниками и зачем.
64. Является ли использование протокола NTLM безопасным и почему?
65. Протокол Kerberos. Дайте определения понятиям: KDC, TGT, TGS.
66. Опишите возможности инструмента Mimikatz.
67. Опишите принцип проведения атаки DCSync.
68. Опишите принцип проведения атаки PTH.
69. Опишите принцип проведения атаки Kerberoasting.
70. Опишите основные принципы «Password Cracking»

Составил
Старший преподаватель кафедры ИБ _____/М.А. Павлунин/

Заведующий кафедрой ИБ _____/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