МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Ф. УТКИНА

Кафедра «Автоматики и информационных технологий в управлении»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность 12.05.01
«Электронные и оптико-электронные приборы
и системы специального назначения»

ОПОП
«Оптико-электронные информационно-измерительные приборы и системы»

Квалификация выпускника – инженер

Формы обучения – очная

Рязань 2021 г.

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 общекультурных, общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся 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, 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 оценки «зачтено – не зачтено». Количество практических работ и их тематика определена рабочей программой дисциплины, утвержденной заведующим кафедрой.

Результат выполнения каждого индивидуального задания должен соответствовать всем критериям оценки в соответствии с компетенциями, установленными для заданного раздела дисциплины.

Промежуточный контроль по дисциплине осуществляется проведением зачета.

Форма проведения зачета – устный ответ по утвержденным вопросам, сформулированным с учетом содержания учебной дисциплины. После устного ответа обучаемого производится оценка его ответа преподавателем по шкале «зачтено – не зачтено» и, при необходимости, проводится теоретическая беседа с обучаемым для уточнения оценки.

Паспорт оценочных материалов по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по темам)	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1	2	3	4
1	**Тема 1. Стохастическая компьютерная вирусология**	ОПК-3.1– З ОПК-3.1– У ОПК-3.1– В ОПК-3.2– З ОПК-3.2– У ОПК-3.2– В	Зачет
2	**Тема 2. Тенденции развития угроз информационной безопасности**	ОПК-3.1– З ОПК-3.1– У ОПК-3.1– В ОПК-3.2– З ОПК-3.2– У ОПК-3.2– В	Зачет
3	**Тема 3. Скрытые каналы передачи данных**	ОПК-3.1– З ОПК-3.1– У ОПК-3.1– В ОПК-3.2– З ОПК-3.2– У ОПК-3.2– В	Зачет
4	**Тема 4. Технология безопасного программирования**	ОПК-3.1– З ОПК-3.1– У ОПК-3.1– В ОПК-3.2– З ОПК-3.2– У ОПК-3.2– В	Зачет

Критерии оценивания компетенций (результатов)

1) Уровень усвоения материала, предусмотренного программой.

2) Умение анализировать материал, устанавливать причинно-следственные связи.

3) Ответы на вопросы: полнота, аргументированность, убежденность, умение

4) Качество ответа (его общая композиция, логичность, убежденность, общая эрудиция)

5) Использование дополнительной литературы при подготовке ответов.

Уровень освоения сформированности знаний, умений и навыков по дисциплине оценивается по шкале **«зачтено – не зачтено»**.

Оценку **«зачтено»** заслуживает студент, 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 «зачтено» выставляется

студентам, допустившим погрешности в ответе на зачете и при выполнении дополнительных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.

Оценка **«не зачтено»** выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий. Как правило, оценка «не зачтено» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Типовые контрольные задания или иные материалы

Вопросы к зачету по дисциплине

1. Чем полиморфные вирусы отличаются от самошифрующихся?
2. Сформулируйте принцип обнаружения компьютерного вируса методом сигнатурного анализа.
3. Сформулируйте принцип обнаружения компьютерного вируса методом эвристического анализа.
4. Какой метод используется для обнаружения компьютерного вируса в момент их активизации?
5. Какой метод используется для обнаружения последствий вирусной активности?
6. Какие методы используются для обнаружения компьютерного вируса до момента их активизации?
7. Какие существуют типы программных средств антивирусной защиты?
8. Что такое вирусная сигнатура? Приведите пример.
9. Что такое эвристический признак компьютерного вируса? Приведите пример.
10. Что такое ошибка 1-го рода при работе программных средств антивирусной защиты?
11. Что такое ошибка 2-го рода при работе программных средств антивирусной защиты?
12. Что такое ошибка 3-го рода при работе программных средств антивирусной защиты?
13. Что такое клептографическая атака на криптоалгоритм?
14. Какие криптоалгоритмы могут являться объектом клептографической атаки?
15. Приведите пример клептографической атаки на криптоалгоритм RSA.
16. Как можно защититься от клептографической атаки?
17. Опишите клептографическую атаку на криптосистему Эль-Гамаля.
18. Опишите возможную клептографическую атаку на генератор ПСЧ.
19. Как вы понимаете термин «клептография»? Приведите примеры, иллюстрирующие данное понятие.
20. Что такое недоказуемое шифрование?
21. Что такое криптовычисления?
22. Каким образом можно получить запись из базы данных таким образом,

чтобы не раскрывать, какая именно запись была получена?
23. Что такое отрицаемое шифрование?
24. Какие программы называют симбиотическими?
25. Приведите примеры симбиотических разрушающих программных воздействий.
26. Каким образом можно использовать сетевые разрушающие программные воздействия для проведения распределенных вычислений?
27. Предположим, что улучшенный криптотроян применяет плохой генератор случайных чисел и сеансовые ключи, сформированные на разных компьютерах, оказываются одинаковыми. Какие последствия это может иметь?
28. Какие методы противодействия автоматической рассылке сообщений вы знаете?
29. В чем различие между принципами недоказуемого и отрицаемого шифрования?
30. Какому риску подвергаются вредоносные программы, участвующие в протоколе информационного шантажа, при использовании ими некачественных генераторов случайных чисел?
31. Какую роль в протоколе контроля работоспособности узлов распределенных вычислений играет случайный бит b?
32. С какой вероятностью для достижения своих целей в протоколе безопасного выкупа жертве придется купить не более k сообщений ($1 \le k \le 2S$)?
33. Дайте определение скрытого канала передачи данных.
34. Дайте определение потайного канала передачи данных.
35. Дайте определение побочного канала передачи данных.
36. Перечислите типы скрытых каналов передачи данных.
37. Что такое скрытый канал по памяти?
38. Что такое скрытый канал по времени?
39. Какие основные характеристики скрытых каналов используются при их описании?
40. Укажите различия между синхронными и асинхронными скрытыми каналами.
41. Какое влияние оказывает синхронизация на емкость канала?
42. Укажите особенности применения скрытых каналов в системах обработки информации.
43. Перечислите методы организации локальных скрытых каналов.
44. Перечислите методы организации сетевых скрытых каналов.
45. Каким образом можно организовать скрытые каналы на базе стека протоколов TCP/IP: IP и ICMP?
46. Каким образом можно организовать скрытые каналы на базе стека протоколов TCP/IP: TCP и UDP?
47. Каким образом можно использовать протоколы уровня приложений HTTP и DNS для организации скрытых каналов?
48. Укажите методы противодействия угрозе организации скрытых каналов?
49. В чем состоят главные отличия компилятора от транслятора?
50. Перечислите преимущества трансляторов?

51. Какие интерпретируемые языки вы знаете?
52. Укажите основные особенности скрипт-вирусов.
53. Укажите методы обнаружения скрипт-вирусов.
54. Какие возможности предоставляет утилита awk?
55. Почему присутствие команды «rm» является одним из наиболее характерных признаков скрипт-вируса?
56. Какими свойствами должен обладать скрипт-файл, чтобы быть классифицированным как вирус?
57. Что такое уязвимость программного кода?
58. К каким последствиям может привести существование уязвимости в программном коде?
59. Каковы основные причины появления уязвимости в программном коде?
60. В чем суть уязвимости, вызванной переполнением буфера на стеке?
61. Укажите основные способы борьбы с уязвимостями переполнения буфера на стеке.
62. К каким последствиям может привести существование уязвимости класса «переполнение кучи»?
63. Укажите основные методы борьбы с уязвимостями класса «переполнение кучи».
64. К каким последствиям может привести существование уязвимостей класса «целочисленное переполнение»?
65. Каковы последствия существования уязвимостей в программах, написанных с использованием интерпретируемых языков?
66. В чем суть уязвимости внедрения команд?
67. К каким последствиям может привести существование уязвимости внедрения SQL-кода?

Практикум по дисциплине

№ п/п	№ темы дисциплины	Наименование практического занятия	Трудоемкость, час
1	1	Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для сокрытия и выполнения деструктивных функций.	2
2	2	Клептографическая атака на алгоритм выработки общего секретного ключа. Защита от клептографических атак.	4
3	3	Классификация скрипт-вирусов. Поиск скрипт-вирусов на основе анализа кода. Выделение эвристических признаков скрипт-вирусов	4
4	4	Уязвимость переполнения буфера. Уязвимость строки формата. Уязвимость целочисленного переполнения. Уязвимость индексации массива. Уязвимость подключения внешних файлов. Уязвимость использования глобальных переменных. Уязвимость внедрения команд. Уязвимость внедрения SQL кода.	6

Типовые задания для самостоятельной работы

1. Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для затруднения своего обнаружения.
2. Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для выполнения деструктивных функций.
3. Элементы теории игр. Информационный шантаж. Распределенные вычисления. Безопасный выкуп.
4. Угроза проведения атак на Unix-системы с использованием скрипт-вирусов для командных интерпретаторов.
5. Интерпретатор и компилятор. Преимущества вирусов на интерпретируемых языках.
6. Скрипт-вирусы на языке Shell. Классификация технических приемов, используемых скрипт-вирусами.
7. Перспективные методы противодействия вредоносным программам.
8. Иммунологический подход к антивирусной защите. Понятие иммунной системы.
9. Архитектура компьютерной иммунной системы.
10. Автономность надежной системы защиты.
11. Стохастический подход к защите информации.
12. Поведенческий анализ программ. Поведение по определению. Определение по поведению.
13. Иммунологический подход. Распределенное обнаружение изменений.
14. Современные тенденции в динамическом анализе кода.