Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Макаренко Елена Николаевна
Должность: Ректор
Дата подписания: 15.11.2024 13:58:57
Уникальный программный ключ:
c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Методы разработки защищенных систем

Направление 09.03.04 "Программная инженерия"
Направленность 09.03.04.01 Системное и прикладное программное обеспечение

Для набора 2022 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по курсам

Курс	3		Итого	
Вид занятий	УП	РП		
Лекции	4	4	4	4
Лабораторные	4	4	4	4
Итого ауд.	8	8	8	8
Контактная работа	8	8	8	8
Сам. работа	96	96	96	96
Часы на контроль	4	4	4	4
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.т.н., доцент, Гунько В.Б.

Зав. кафедрой: к.э.н. Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	формирование компетентности в области разработки защищённых систем, отдельных компонентов информационных систем, с учётом требований нормативно-технической и методической документации по обеспечению безопасности информации

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-4: способен формировать цели и бизнес-требования, осуществлять постановку задач, планировать разработку, оценивать начальную степень трудности и риски, составлять техническое задание и шаблоны документов требований к подсистемам системы и контроль их качества (в том числе атрибуты надежности, безопасности, удобства использования)

ПК-3: способен разрабатывать компоненты программных комплексов (в том числе интерфейсы, драйвера, компиляторы, загрузчики, сборщики, системные утилиты) и баз данных с использованием современных инструментальных средств и технологий программирования

В результате освоения дисциплины обучающийся должен:

Знать:

основы информатики и программирования; (соотнесено с индикатором ПК-3.1)
современные информационные технологии и возможности их применения в бизнесе. (соотнесено с индикатором ПК-4.1)

Уметь:

использовать современные технологии разработки программных продуктов; (соотнесено с индикатором ПК-3.2)
использовать информационные технологии для оптимизации бизнеса. (соотнесено с индикатором ПК-4.2)

Владеть:

навыками разработки алгоритмов в виде блок-схемы и составления плана ручного тестирования разрабатываемого программного продукта; (соотнесено с индикатором ПК-3.3)
навыками эффективного использования информационных технологий при решении профессиональных задач. (соотнесено с индикатором ПК-4.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Теоретические вопросы разработки программного кода

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Основные понятия, определения и проблемы в области разработки защищённых систем / Лек /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.2	Обзор и сравнительный анализ стандартов в области защиты информационных систем / Ср /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.3	Исследование причин нарушений безопасности информационных систем / Ср /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.4	Анализ и оценка информационных рисков, угрозы и уязвимости информационной системы / Лек /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.5	Специальные методы моделирования, используемые при разработке защищённых систем / Ср /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.6	Методы принятия решений, используемые при выборе эффективных проектов защиты информации в информационной системе / Ср /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.7	Технология Data Mining для поддержки принятия решений при разработке защищённых систем / Ср /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.8	Технология OLAP для визуализаций решений при разработке защищённых систем / Ср /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.9	Перспективные направления в области разработки защищённых систем / Ср /	3	6	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 2. Практика разработки защищенного программного кода					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
2.1	Формальные модели представления защищённых информационных систем. Assembler / Ср /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.2	Инструментальные средства проектирования. Графические средства представления проектных решений. Методология IDEF / Ср /	3	2	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.3	Инструментальные средства проектирования. Графические средства представления проектных решений. Методология DFD / Ср /	3	4	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.4	Инструментальные средства проектирования. Графические средства представления проектных решений. Методология eEPC и UML / Ср /	3	4	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.5	Инструментальные средства проектирования. Графические средства представления проектных решений. Технологии CAD/CAE/CAM / Ср /	3	4	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.6	Анализ рисков при разработке защищённых информационных систем / Ср /	3	4	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.7	Основы UML – диаграмма вариантов использования / Лаб /	3	4	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.8	Использование диаграммы классов UML для описания защищённой информационной системы / Ср /	3	4	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.9	Использование диаграммы последовательности UML для описания защищённой информационной системы / Ср /	3	4	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
Раздел 3. Теоретические вопросы создания проекта защищенных систем					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
3.1	Проработка лекционного материала. Основные понятия, определения и проблемы в области разработки защищённых систем / Ср /	3	18	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
3.2	Обзор и сравнительный анализ стандартов в области защиты информационных систем / Ср /	3	18	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
3.3	Исследование причин нарушений безопасности информационных систем / Ср /	3	14	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
3.4	/ Зачёт /	3	4	ПК-4, ПК-3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Голиков А. М.	Защита информации в инфокоммуникационных системах и сетях: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2015	https://biblioclub.ru/index.php?page=book&id=480637 неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.2	Лисяк, В. В.	Разработка информационных систем: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2019	https://www.iprbookshop.ru/95818.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Рак, И. П., Платёнкин, А. В., Терехов, А. В.	Основы разработки информационных систем: учебное пособие	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2017	https://www.iprbookshop.ru/85939.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Титов А. А.	Инженерно-техническая защита информации: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010	https://biblioclub.ru/index.php?page=book&id=208567 неограниченный доступ для зарегистрированных пользователей
Л2.2	Свинарев Н. А., Ланкин О. В., Данилкин А. П., Потехецкий С. В., Перетокин О. И.	Инструментальный контроль и защита информации: учебное пособие	Воронеж: Воронежский государственный университет инженерных технологий, 2013	https://biblioclub.ru/index.php?page=book&id=255905 неограниченный доступ для зарегистрированных пользователей
Л2.3		Информационные системы и технологии: журнал	Орел: Госуниверситет - УНПК, 2015	https://biblioclub.ru/index.php?page=book&id=446338 неограниченный доступ для зарегистрированных пользователей
Л2.4	Голиков А. М.	Защита информации от утечки по техническим каналам: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2015	https://biblioclub.ru/index.php?page=book&id=480636 неограниченный доступ для зарегистрированных пользователей
Л2.5		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2018	https://biblioclub.ru/index.php?page=book&id=562403 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

ФСТЭК РФ/fstec.ru
Образовательный портал "Основы программирования на языках Си и С++ для начинающих" - http://cppstudio.com/
Консультант +

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
Assembler

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной

учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-3 – способен разрабатывать компоненты программных комплексов (в том числе интерфейсы, драйвера, компиляторы, загрузчики, сборщики, системные утилиты) и баз данных с использованием современных инструментальных средств и технологий программирования			
З. основы информатики и программирования	знает программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования при подготовке к опросу и зачету	сформировавшееся систематическое знание программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования при ответе на вопросы опроса и зачета	О (вопросы 1-60), З (вопросы 1-60)
У. использовать современные технологии разработки программных продуктов	использует программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования при выполнении лабораторных и практико-ориентированных заданий	сформировавшееся систематическое умение использования программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования при выполнении лабораторных и практико-ориентированных заданий	ЛЗ (ЛЗ 1- ЛЗ 9); ПОЗЗ (задание 1-6)
В навыками разработки алгоритмов в виде блок-схемы и составления плана ручного тестирования разрабатываемого программного продукта	владеет навыками применения программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования при выполнении лабораторных и практико-ориентированных заданий	сформировавшееся систематическое владение навыками применения программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования при выполнении лабораторных и практико-ориентированных заданий	ЛЗ (ЛЗ 1- ЛЗ 9); ПОЗЗ (задание 1-6)
ПК-4 – способен формировать цели и бизнес-требования, осуществлять постановку задач, планировать разработку, оценивать начальную степень трудности и риски, составлять техническое задание и шаблоны документов требований к подсистемам системы и контроль их качества (в том числе атрибуты надежности, безопасности, удобства использования)			
З. современные информационные технологии и возможности их применения в бизнесе	знает современные информационные технологии и возможности их применения в бизнесе при подготовке к опросу и зачету	сформировавшееся систематическое знание современных информационных технологий и возможностей их применения в бизнесе при ответе на вопросы опроса и зачета	О (вопросы 1-60), З (вопросы 1-60)
У. использовать информационные технологии для оптимизации бизнеса	Использует информационные технологии для оптимизации бизнеса при выполнении лабораторных и практико-ориентированных заданий	корректность использования информационных технологий для оптимизации бизнеса при выполнении лабораторных и практико-ориентированных заданий	ЛЗ (ЛЗ 1- ЛЗ 9); ПОЗЗ (задание 1-6)
В. навыками эффективного использования информационных технологий при решении профессиональных задач	владеет навыками эффективного использования информационных технологий при выполнении лабораторных и практико-ориентированных заданий	сформировавшееся систематическое владение навыками эффективного использования информационных технологий при выполнении лабораторных и практико-ориентированных заданий	ЛЗ (ЛЗ 1- ЛЗ 9); ПОЗЗ (задание 1-6)

О – опрос, ЛЗ – лабораторные задания, ПОЗЗ - практико-ориентированные задания к зачету, З- вопросы к зачету.

1.2 Шкалы оценивания:
Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале.
- 50-100 баллов (зачет);
- 0-49 баллов (не зачет).

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1. Основное отличие вируса от любого другого программного кода
2. Основные свойства вируса, определяющие его живучесть
3. Характеристики компьютерного вируса, соответствующие характеристикам биологического
4. Среда функционирования компьютерного вируса
5. Методы внедрения вируса в объекты информационной системы
6. Классификация вирусов по объектам заражения
7. Определение свойства резидетности вируса
8. Понятие MBR и ее роль в распространении вирусов
9. Методы маскировки компьютерных вирусов
10. Свойство полиморфности компьютерных вирусов
11. Недостатки полиморфных вирусов
12. Достоинства полиморфных вирусов
13. Определение Stealth-вирусов и их основные свойства
14. Недостатки Stealth- вирусов
15. Достоинства Stealth-вирусов
16. Понятие перехвата функций ОС, как алгоритма работы вирусов
17. Классификация троянских программ
18. Среда распространения компьютерных червей
19. Особенности функционирования эксплоитов.
20. Методы обнаружения вирусной инвазии
21. Признаки заражения информационной системы
22. Признаки заражения исполняемых файлов
23. Признаки заражения неисполняемых файлов
24. Достоинства сигнатурных методов обнаружения вирусов
25. Недостатки сигнатурных методов обнаружения вирусов
26. Достоинства не сигнатурных методов обнаружения вирусов
27. Недостатки не сигнатурных методов обнаружения вирусов
28. Тип вирусов, имеющий максимальную инфицирующую способность
29. Определение статического метода анализа исполняемого кода
30. Определение динамического метода анализа исполняемого кода
31. Параметры воздействия сетевой атаки на внешний периметр информационной системы
32. Параметры воздействия сетевой атаки на внутренний периметр информационной системы
33. Этапы проведения сетевой атаки
34. Определение самого сложного по реализации этапа сетевой атаки
35. Цели сетевой удаленной атаки
36. Методы анализа атакуемого узла
37. Классификация удаленных атак по уровню воздействия на атакуемые объекты
38. Сущность атаки типа Sniffing
39. Сущность атаки типа Spoofing
40. Основные проблемы при реализации атаки типа Spoofing
41. Сущность атаки типа Hijacking

42. Основные проблемы при проведении атаки типа Hijacking
43. Классификация атак типа Инъекция
44. Основные причины возможности проведения атаки типа Инъекция
45. Алгоритм поведения атаки типа Иньекция на скрипт-коды
46. Алгоритм проведения атаки типа SQL-инъекция
47. Классификация XSS атак
48. Отличия между хранимой и временной XSS атаками
49. Понятия и сущность Flood-атаки
50. Различия между DoS и DDoS атаками
51. Методы проведения DNS-атак
52. Сущность атаки ICMP-флуд (Smurf)
53. Сущность атаки UDP-флуд (Fraggle)
54. Особенности проведения атаки по переполнению буфера
55. Сущность атаки SYN-флуд
56. Методы проведения атаки BruteForce
57. Условия успешного проведения атак типа DoS/DDoS/Flood
58. Причины актуальности сетевых удаленных атак
59. Сущность активного сканирования атакуемого сетевого ресурса
60. Сущность пассивного сканирования атакуемого сетевого ресурса

Практико-ориентированные задания к зачету

Задание 1 Заданы: - когнитивная карта G(V, W), где V - множество вершин (факторов ситуации), W - матрица смежности; - множество {Z1, …, Zn} шкал всех факторов ситуации; - начальное состояние ситуации X(0)=(x1(0), …, xn(0)); - начальный вектор приращений факторов ситуации P(0)=(p1(0),…, pn(0)). Необходимо найти состояния ситуации X(1), … , X(n) и векторы приращений P(1), … , P(n) в последовательные дискретные моменты времени {1, … , n}, где n=|| V || для того, чтобы влияние исходного возмущения могло достичь всех вершин.
Задание 2 Используя программное обеспечение для сканирования сетей, определить уязвимости хоста.
Задание 3 Создать защищённое соединения с применением доступного программного обеспечения.
Задание 4 - Разработать модель потенциальных угроз.
Задание 5 Используя одну из стандартных методик провести оценку рисков и сформировать на её основе список актуальных угроз.
Задание 6 Разработать одну из политик безопасности для данного объекта.

Зачетное задание включает 2 теоретических вопроса (раздел «Вопросы к зачету») и 1 практико-ориентированное задание (формируется из перечня заданий, представленных в разделе «Практико-ориентированные задания к зачету»).

Критерии оценивания:
Максимальное количество баллов за зачетное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:
1 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
2 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;

3 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
4 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:
1. 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
2. 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
3. 11-24 балла выставляется, если задание решено частично.
4. 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:
1. 50-100 баллов (зачтено);
2. 0-49 баллов (не зачтено).

Лабораторные задания

Раздел 2 «Практика разработки защищенного программного кода».
Лабораторное задание 1 Формальные модели представления защищённых информационных систем. Assembler
Лабораторное задание 2 Инструментальные средства проектирования. Графические средства представления проектных решений. Методология IDEF
Лабораторное задание 3 Инструментальные средства проектирования. Графические средства представления проектных решений. Методология DFD.
Лабораторное задание 4 Инструментальные средства проектирования. Графические средства представления проектных решений. Методология eEPC и UML.
Лабораторное задание 5 Инструментальные средства проектирования. Графические средства представления проектных решений. Технологии CAD/CAE/CAM.
Лабораторное задание 6 Анализ рисков при разработке защищённых информационных систем.
Лабораторное задание 7 Основы UML – диаграмма вариантов использования.
Лабораторное задание 8 Использование диаграммы классов UML для описания защищённой информационной системы.
Лабораторное задание 9 Использование диаграммы последовательности UML для описания защищённой информационной системы.
Критерии оценивания:
Максимальное количество баллов: 72 балла.
Каждое задание оценивается максимум в 8 баллов.
8 б. – задание выполнено верно;
7-6 б. – при выполнении задания были допущены неточности, не влияющие на результат;
5-4 б. – при выполнении задания были допущены ошибки;
3-1 б. – при выполнении задания были допущены существенные ошибки.
0 б. – задание не выполнено.

Вопросы для опроса

1. Основное отличие вируса от любого другого программного кода
2. Основные свойства вируса, определяющие его живучесть
3. Характеристики компьютерного вируса, соответствующие характеристикам биологического
4. Среда функционирования компьютерного вируса
5. Методы внедрения вируса в объекты информационной системы

6. Классификация вирусов по объектам заражения
7. Определение свойства резидетности вируса
8. Понятие MBR и ее роль в распространении вирусов
9. Методы маскировки компьютерных вирусов
10. Свойство полиморфности компьютерных вирусов
11. Недостатки полиморфных вирусов
12. Достоинства полиморфных вирусов
13. Определение Stealth-вирусов и их основные свойства
14. Недостатки Stealth- вирусов
15. Достоинства Stealth-вирусов
16. Понятие перехвата функций ОС, как алгоритма работы вирусов
17. Классификация троянских программ
18. Среда распространения компьютерных червей
19. Особенности функционирования эксплоитов.
20. Методы обнаружения вирусной инвазии
21. Признаки заражения информационной системы
22. Признаки заражения исполняемых файлов
23. Признаки заражения неисполняемых файлов
24. Достоинства сигнатурных методов обнаружения вирусов
25. Недостатки сигнатурных методов обнаружения вирусов
26. Достоинства не сигнатурных методов обнаружения вирусов
27. Недостатки не сигнатурных методов обнаружения вирусов
28. Тип вирусов, имеющий максимальную инфицирующую способность
29. Определение статического метода анализа исполняемого кода
30. Определение динамического метода анализа исполняемого кода
31. Параметры воздействия сетевой атаки на внешний периметр информационной системы
32. Параметры воздействия сетевой атаки на внутренний периметр информационной системы
33. Этапы проведения сетевой атаки
34. Определение самого сложного по реализации этапа сетевой атаки
35. Цели сетевой удаленной атаки
36. Методы анализа атакуемого узла
37. Классификация удаленных атак по уровню воздействия на атакуемые объекты
38. Сущность атаки типа Sniffing
39. Сущность атаки типа Spoofing
40. Основные проблемы при реализации атаки типа Spoofing
41. Сущность атаки типа Hijacking
42. Основные проблемы при проведении атаки типа Hijacking
43. Классификация атак типа Инъекция
44. Основные причины возможности проведения атаки типа Инъекция
45. Алгоритм поведения атаки типа Иньекция на скрипт-коды
46. Алгоритм проведения атаки типа SQL-инъекция
47. Классификация XSS атак
48. Отличия между хранимой и временной XSS атаками
49. Понятия и сущность Flood-атаки
50. Различия между DoS и DDoS атаками
51. Методы проведения DNS-атак
52. Сущность атаки ICMP-флуд (Smurf)
53. Сущность атаки UDP-флуд (Fraggle)
54. Особенности проведения атаки по переполнению буфера
55. Сущность атаки SYN-флуд
56. Методы проведения атаки BruteForce
57. Условия успешного проведения атак типа DoS/DDoS/Flood
58. Причины актуальности сетевых удаленных атак
59. Сущность активного сканирования атакуемого сетевого ресурса
60. Сущность пассивного сканирования атакуемого сетевого ресурса

Критерии оценивания:
Максимальное количество баллов: 28 баллов.
Во время опроса обучаемому задаются 7 вопросов.
За один ответ обучаемый получает:
4 б. – за правильный ответ;
3 б. – при ответе были допущены неточности, не влияющие на результат;
2 б. – при ответе были допущены ошибки;
1 б. – при ответе были допущены существенные ошибки.
0 б. – не ответил на вопрос.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.
Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.
Промежуточная аттестация проводится в форме зачета.
Зачет проводится по окончанию теоретического обучения до начала экзаменационной сессии в соответствии с расписанием. Количество вопросов в задании – 3: два теоретических вопроса и одно практико-ориентированное задание. Объявление результатов производится в день зачета. Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:
- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные теоретические вопросы, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

При подготовке к лабораторным занятиям каждый студент должен:
– изучить рекомендованную учебную литературу;
– изучить конспекты лекций;
– подготовить ответы на все вопросы по изучаемой теме.

В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом опроса. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему лабораторному занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.