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

УТВЕРЖДАЮ
Первый проректор –
проректор по учебной работе
____________ Н.Г. Кузнецов
«01» июня 2018г.

Рабочая программа дисциплины

Защита от удаленных сетевых атак

по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Квалификация

Бакалавр

Ростов-на-Дону
2018 г.

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Недель	17,3			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Лабораторные	18	18	18	18
В том числе инт.	18	18	18	18
Итого ауд.	36	36	36	36
Контактная	36	36	36	36
Сам. работа	72	72	72	72
Итого	108	108	108	108

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 "Информационная безопасность" (уровень бакалавриата) (приказ Минобрнауки России от 01.12.2016г. №1515)

Рабочая программа составлена по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Учебный план утвержден учёным советом вуза от 27.03.2018 протокол № 10.

Программу составил(и): д.э.н., зав. кафедрой, Тищенко Е. Н. _____ 10.05.2018

Зав. кафедрой: д.э.н., профессор Тищенко Е.Н. _____ 11.05.2018

Методическим советом направления: к.ф.-м.н., Карасев Д.Н. _____ 29.05.2018

Отделом образовательных программ и планирования учебного процесса Торопова Т.В. _____ 30.05.2018

Проректором по учебно-методической работе Джуха В.М. _____ 31.05.2018

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2019-2020 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): д.э.н., зав. кафедрой, Тищенко Е. Н. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2020-2021 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): д.э.н., зав. кафедрой, Тищенко Е. Н. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): д.э.н., зав. кафедрой, Тищенко Е. Н. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): д.э.н., зав. кафедрой, Тищенко Е. Н. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цели дисциплины. Изучение дисциплины "Защита от удаленных сетевых атак" направлено на достижение следующих целей: развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением защищенности информационных систем от удаленных сетевых атак; развитие профессиональных компетенций для нахождения оптимальных решений при построении защищенных информационных систем; привитие навыков использования специализированных средств защиты.
1.2	Задачи дисциплины. Дать знания по вопросам: обеспечения защиты от удаленных сетевых атак; методологии создания систем защиты от удаленных сетевых атак; процессов сбора, передачи и накопления при защите от удаленных сетевых атак; методов и средств защиты от удаленных сетевых атак; оценки защищенности и обеспечения информационной безопасности компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.В.ДВ.03
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Необходимыми условиями для успешного освоения являются навыки, знания и умения, полученные в результате освоения дисциплин:
2.1.2	Информационная безопасность в системах электронной коммерции
2.1.3	Методы атакующего воздействия на информационные ресурсы
2.1.4	Средства и методы защиты хранилищ и баз данных
2.1.5	Основы информационной безопасности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Комплексное обеспечение защиты информации объекта информатизации
2.2.2	Моделирование процессов и систем защиты информации
2.2.3	Основы управления информационной безопасностью

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Знать:
основные методы по установке, настройке и обслуживанию средств защиты информации на базовом уровне
Уметь:
применять основные методы по установке, настройке и обслуживанию средств защиты информации на базовом уровне
Владеть:
навыками использования специальных средств защиты информации на базовом уровне
ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты
Знать:
основные методы администрирования подсистем информационной безопасности на базовом уровне
Уметь:
применять методы администрирования подсистем информационной безопасности на базовом уровне
Владеть:
навыками администрирования подсистем информационной безопасности на базом уровне

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Интер акт.	Примечание
	Раздел 1. Основные понятия и определения						
1.1	Понятие удаленной сетевой атаки: виды виды сетевых атак; уязвимости информационных систем при реализации сетевой атаки; внешний и внутренний периметры /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	2	
1.2	Понятие понятие удаленной сетевой атаки: лабораторные занятия по теме лекции /Лаб/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	0	

1.3	Понятие понятие удаленной сетевой атаки: самостоятельная работа по теме лекции /Ср/	6	8	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	0	
1.4	Методы защиты от удаленных сетевых атак: криптографические методы, межсетевые экраны, системы обнаружения атак /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	2	
1.5	Виды защищаемой информации: лабораторные занятия по теме лекции /Лаб/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	0	
1.6	Методы защиты от удаленных сетевых атак: самостоятельная работа по теме лекции /Ср/	6	8	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	0	
	Раздел 2. Классификация удаленных сетевых атак						
2.1	Атаки типа "отказ в обслуживании": простые атаки, распределенные атаки, атаки типа "шторм" /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	2	
2.2	Атаки типа "отказ в обслуживании":практические занятия по теме лекции. /Лаб/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	0	
2.3	Атаки типа "отказ в обслуживании": самостоятельная работа по теме лекции /Ср/	6	8	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	0	
2.4	Атака типа "иньекция": PHP-иньекция, SQL-иньекция, JAVA-иньекция, межсайтовый скриптинг /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	2	
2.5	Атака типа "иньекция": практические занятия по теме лекции /Лаб/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1	0	
2.6	Атака типа "иньекция": самостоятельная работа по теме лекции /Ср/	6	8	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.7	Атака типа "Spoofing": подмена MAC-адреса, подмена IP-адреса, подмена DNS-адреса /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.8	Атака типа "Spoofing": лабораторные занятия по теме лекции /Лаб/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	2	
2.9	Атака типа "Spoofing": самостоятельные занятия по теме лекции /Ср/	6	8	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.10	Пассивные атаки: атака типа "Sniffing", атака с использованием комлексных средств анализа трафика /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.11	Пассивные атаки: лабораторные занятия по теме лекции /Лаб/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	2	
2.12	Пассивные атаки: самостоятельная работа по теме лекции /Ср/	6	8	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
	Раздел 3. Методы и средства защиты от удаленных сетевых атак						

3.1	Межсетевое экранирование: персональные и корпоративные межсетевые экраны, программные и аппаратные межсетевые экраны, классификация экранов по стеку TCP/IP /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.2	Межсетевое экранирование: лабораторные занятия по теме лекции /Лаб/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	2	
3.3	Межсетевое экранирование: самостоятельная работа по теме лекции /Ср/	6	8	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.4	Криптографические методы: VPN, скремблирование, туннелирование /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.5	Криптографические методы: лабораторные занятия по теме лекции /Лаб/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	2	
3.6	Криптографические методы: самостоятельная работа по теме лекции /Ср/	6	8	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.7	Ситемы обнаружения уязвимостей: IDS-системы, IPS-системы /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.8	Системы обнаружения уязвимостей: лабораторные занятия по теме лекции /Лаб/	6	2	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	2	
3.9	Системы обнаружения уязвимостей: самостоятельная работа по теме лекции по теме лекции /Ср/	6	8	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.10	/Зачёт/	6	0	ПК-1 ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

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

5.2. Фонд оценочных средств для проведения текущего контроля

Структура и содержание фонда оценочных средств представлены в Приложении 1 к рабочей программе дисциплины

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А.	Информационная безопасность и защита информации: учеб. пособие для студентов вузов, обучающихся по спец. "Информ. системы и технологии"	М.: Академия, 2012	20
Л1.2	Рытенкова О.	Информационная безопасность	Москва: ГРОТЕК, 2014	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Мельников Д. А.	Информационная безопасность открытых систем: учеб. для студентов, обучающихся по напр. "Приклад. информатика"	М.: Флинта, 2013	20

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.2		Информационная безопасность	Москва: Гротек, 2014	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Тищенко Е. Н.	Инструментальные методы анализа потребительского качества защищенных информационных систем: учеб. пособие	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2016	68

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	ФСТЭК России/fstec.ru

6.3. Перечень программного обеспечения

6.3.1	Анализатор уязвимостей XSpider
6.3.2	Анализатор уязвимостей MaxPatrol
6.3.3	Межсетевой экран PFSense
6.3.4	Удостоверяющий центр VipNet

6.4 Перечень информационных справочных систем

6.4.1	Consultant Plus

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по усвоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины

Приложение 1
к рабочей программе

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

Рассмотрено и одобрено
на заседании кафедры Информационных
технологий и защиты информации
Протокол №10 от «12» мая 2018 г.
Зав.кафедрой _____ *Тищенко Е.Н.*

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Б.1.В.ДВ.3.1 «Защита от удаленных сетевых атак»
(наименование дисциплины)

Направление подготовки

10.03.01 «Информационная безопасность»

Уровень образования
бакалавриат

Составитель _____ Тищенко Е.Н., профессор, д.э.н.
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Оглавление

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

1.1 Перечень компетенций с указанием этапов их формирования представлен в п. 3. «Требования к результатам освоения дисциплины» рабочей программы дисциплины.

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

2.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-1 – способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации			
З: основные методы по установке, настройке и обслуживанию средств защиты информации	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа, Т - тест
У: применять основные методы по установке, настройке и обслуживанию средств защиты информации	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа , Т - тест

В: навыками использования специальных средств защиты информации	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа, Т - тест
ПК-3 – способность администрировать подсистемы информационной безопасности объекта защиты			
З: основные методы администрирования подсистем информационной безопасности	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа, Т - тест
У: применять методы администрирования подсистем информационной безопасности	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа, Т - тест
В: навыками администрирования подсистем информационной безопасности	поиск и сбор необходимой литературы, использование различных баз данных, использование	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры;	ЛР – лабораторная работа , Т - тест

	современных информационно-коммуникационных технологий и глобальных информационных ресурсов	умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	

2.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале.

- 84-100 баллов (оценка «отлично») - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 67-83 баллов (оценка «хорошо») - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- 50-66 баллов (оценка удовлетворительно) - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 баллов (оценка неудовлетворительно) - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

3 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

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования

«Ростовский государственный экономический университет (РИНХ)»

Кафедра Информационных технологий и защиты информации
(наименование кафедры)

Вопросы к экзамену

по дисциплине «Защита от удаленных сетевых атак»
(наименование дисциплины)

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:

- оценка «отлично» - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

оценка «хорошо» - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- оценка удовлетворительно - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных

вопросов; правильные в целом действия по применению знаний на практике;

- оценка неудовлетворительно - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

Оформление лабораторных работ

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

Кафедра Информационных технологий и защиты информации
(наименование кафедры)

Лабораторные работы

по дисциплине «Защита от удаленных сетевых атак»
(наименование дисциплины)

1. Методические рекомендации по выполнению лабораторных работ

Лабораторная работа как вид учебного занятия проводиться в специально оборудованных учебных аудиториях.

Продолжительность не менее 2-х академических часов. Необходимыми структурными элементами лабораторной работы, помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

Выполнению лабораторной работы предшествует проверка знаний студентов, их теоретической готовности к выполнению задания.

По каждой лабораторной работе преподаватели должны разработать методические указания по их проведению, в соответствии с требованиями их оформления.

2. Критерии оценки:

«зачтено» выставляется студенту, если задание, предусмотренное лабораторной работой, выполнено на компьютере и студент может объяснить ее выполнение;

- «не зачтено» - выставляется студенту, если задание, предусмотренное лабораторной работой, не выполнено на компьютере или он не может объяснить ее выполнение.

4 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. 3 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном задании – 3. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2
к рабочей программе

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

Рассмотрено и одобрено
на заседании кафедры
Информационных технологий и защиты информации
Протокол №10 от «12» мая 2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б.1.В.ДВ.3.1 «Защита от удаленных сетевых атак»
(наименование дисциплины)

Направление подготовки

10.03.01 «Информационная безопасность»

Уровень образования
бакалавриат

Составитель _____ Тищенко Е.Н., д.э.н., профессор
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Защита от удаленных сетевых атак» адресованы студентам всех форм обучения.

Учебным планом по направлению подготовки «Информационная безопасность» предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия и методы по дисциплине Защита от удаленных сетевых атак, даются рекомендации для самостоятельной работы и подготовке к практическим занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач дисциплины.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы, помещённые в конце описания лабораторной работы.

Вопросы, не рассмотренные на лекциях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины осуществляется в ходе занятий методом устного опроса, проверки выполненных индивидуальных заданий, тестирования, проверки подготовленных конспектов по выделенным для самостоятельного изучения темам дисциплины. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных, выделить непонятные термины и найти их значение в энциклопедических словарях.

При реализации различных видов учебной работы используются разнообразные (в т.ч. интерактивные) методы обучения, в частности:

- размещение материалов курса в системе дистанционного обучения http://elearning.rsue.ru/

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронной библиотекой ВУЗа http://library.rsue.ru/. Также обучающиеся могут взять на дом необходимую литературу на абонементе вузовской библиотеки или воспользоваться читальными залами вуза.