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

Теория информационной безопасности и методология защиты информации

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>)	**5 (3.1)**		Итого	
Недель	17,3			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Лабораторные	36	36	36	36
В том числе инт.	16	16	16	16
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	54	54	54	54
Часы на контроль	36	36	36	36
Итого	144	144	144	144

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): к.т.н. , доцент, Скляров А.В. _____ 10.05.18

Зав. кафедрой: д.э.н. Тищенко Е.Н. _____ 11.05.18

Методическим советом направления: к.ф-м.н., доцент, Карасев Д.Н. _____ 15.05.18

Отделом образовательных программ и планирования учебного процесса Торопова Т.В. _____ 30.05.18

Проректором по учебно-методической работе Джуха В.М. _____ 31.05.18

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. Тищенко Е.Н. _____

Программу составил(и): к.ф-м.н.

, доцент, Карасев Л.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. Тищенко Е.Н. _____

Программу составил(и): к.ф-м.н.

, доцент, Карасев Л.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. Тищенко Е.Н. _____

Программу составил(и): к.ф-м.н.

, доцент, Карасев Л.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. Тищенко Е.Н. _____

Программу составил(и): к.ф-м.н.

, доцент, Карасев Л.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цель дисциплины – изучить теоретические основы информационной безопасности (ИБ) и методологические нормы системного обеспечения защиты информационных процессов в компьютерных системах.
1.2	Теория определяется как совокупность основных идей и общих принципов, объединенных в единую систему и обобщенно раскрывающих ту или другую область действительности.
1.3	Применительно к ИБ теорию следует рассматривать как систему основных идей и положений, общих принципов, необходимых для раскрытия сущности и значения ИБ и выработки методологии ЗИ в компьютерных системах.
1.4	Методология ЗИ в компьютерных системах - это учение о структуре, логической организации системы ЗИ, видах, методах и средствах деятельности по обеспечению безопасности защищаемой информации в компьютерных системах.
1.5	Задачи дисциплины:
1.6	-раскрытие понятийного аппарата в области ИБ и ЗИ в компьютерных системах;
1.7	-раскрытие содержательных базовых положений;
1.8	-раскрытие современной доктрины ИБ;
1.9	-определение целей и принципов ЗИ в компьютерных системах;
1.10	-установление факторов, влияющих на ЗИ;
1.11	-установление угроз информации в компьютерных системах;
1.12	-раскрытие направлений, видов, методов и особенностей деятельности злоумышленников в компьютерной сети и при наличии изолированного компьютера;
1.13	-раскрытие назначения, сущности и структуры системы ЗИ в компьютерных системах, системных вопросов защиты программ и данных;
1.14	-определение требований к программной и программно-аппаратной реализации средств ЗИ в компьютерных системах и к защите АСУ от несанкционированного доступа (НСД).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.Б
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Для успешного освоения дисциплины студент должен иметь базовую подготовку по физике и математике
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Информационная безопасность в системах электронной коммерции
2.2.2	Методы и средства обеспечения информационной безопасности
2.2.3	Защита информационных процессов и систем
2.2.4	Комплексное обеспечение защиты информации объекта информатизации

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
Знать:
Уметь:
Владеть:
ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты
Знать:
Принципы построения и функционирования подсистемы информационной безопасности объекта защиты
Уметь:
Осуществлять научно обоснованный выбор способов администрирования подсистемы информационной безопасности объекта защиты
Владеть:
Методиками научно обоснованного выбора способов администрирования подсистемы информационной безопасности объекта защиты.
ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

Знать:
основы комплексного подхода к обеспечению информационной безопасности объекта защиты
Уметь:
Осуществлять научно обоснованный выбор методов практической реализации политики информационной безопасности
Владеть:
Методиками научно обоснованного вы-бора методов практической реализации политики информационной безопасности

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 составляющие информационной безопасности						
1.1	Основные составляющие ИБ. Основные принципы обеспечения ИБ Безопасность в информационном обществе Информация в современном мире и её свойства Понятие безопасности /Лек/	5	2	ПК-3	Л1.1	0	
1.2	Структура органов РФ по обеспечению ИБ. Информационная война как угроза национальной бе¬зопасности Место информационной безопасности в системе нацио¬нальной безопасности Значение информационной безопасности для субъектов	5	4	ПК-3 ПК-4	Л1.1	0	
1.3	Разработка программы псевдослучайной генерации чисел.Методы генерации кодов .Расчет стойкости кодов. /Лаб/	5	6	ПК-3 ПК-4	Л1.1	0	
1.4	Основные составляющие информационной безопасности Целосность Доступность Конфеденциальность. /Ср/	5	4	ПК-3 ПК-4	Л1.1 Л2.1	0	
	Раздел 2. Теоретические основы информационной безопасности.						
2.1	Концептуальная модель информационной безопасности РФ. Концептуальная модель и основные понятия Объекты и угрозы информационной безопасности России Политика обеспечения информационной безопасности Российской Федерации /Лек/	5	2	ПК-4	Л1.1	1	
2.2	Система обеспечения информационной безопасности РФ. Концептуальная модель и основные понятия Объекты и угрозы информационной безопасности России Политика обеспечения информационной безопасности	5	4	ПК-3 ПК-4	Л1.1	0	
2.3	Система обеспечения информационной безопасности организации Концептуальная модель и основные понятия Объекты и угрозы информационной безопасности организации Политика обеспечения информационной безопасности организации. /Ср/	5	4	ПК-3	Л1.1	0	
2.4	Разработка программы антивируса-монитора Панятие антивируса-монитора Создание программы Отладка программы Исследование программы /Лаб/	5	6	ПК-3 ПК-4	Л1.1	0	

	Раздел 3. Понятие и сущность защиты информации.						
3.1	Цели и задачи защиты информации.Общий контекст защиты информации Понятие и сущность защиты информации как вида деятельности Цели и задачи защиты информации Концептуальная модель защиты информации /Лек/	5	2	ПК-3 ПК-4	Л1.1 Л2.1	1	
3.2	Понятие и сущность защиты информации как вида деятельности. 6.1 Основные положения теории защиты информации Модели систем и процессов защиты информации /Лек/	5	2	ПК-4	Л1.1 Л2.1	1	
3.3	Основные положения теории защиты ин -формации Общий контекст защиты информации Понятие и сущность защиты информации как вида деятельности Цели и задачи защиты информации Концептуальная модель защиты информации /Ср/	5	4	ПК-3 ПК-4	Л1.1 Л2.1	0	
3.4	Состав и основные свойства защищаемой информации Основные свойства информации, обуславливающие необходимость её защиты Понятие и состав защищаемой информации. Принци¬пы отнесения информации к защищаемой Носители защищаемой информации /Ср/	5	4	ПК-3 ПК-4	Л1.1 Л2.1	0	
3.5	Разработка программы имитирующей вирусоподобные действия СозданНие модели Отладка программы Исследование программы /Лаб/	5	6	ПК-3 ПК-4	Л1.1 Л2.1	2	
3.6	Понятие и сущность защиты информации. Понятие и сущность защиты информации как вида деятельности Цели и задачи защиты информации Концептуальная модель защиты информации /Ср/	5	4	ПК-3 ПК-4	Л1.1 Л2.1	0	
	Раздел 4. Понятие, классификация и оценка угроз безопасности информации						
4.1	Понятие угрозы и её взаимосвязь с уязвимостью и рисками. Понятие угрозы и её взаимосвязь с уязвимостью и рисками Общая классификация угроз безопасности информации Цели и задачи оценки угроз безопасности информации /Лек/	5	2	ПК-3	Л1.1 Л2.1	1	
4.2	Источники и способы реализации угроз безопасности информации. Понятие угрозы и её взаимосвязь с уязвимостью и рисками Общая классификация угроз безопасности информации Цели и задачи оценки угроз безопасности информации /Ср/	5	6	ПК-3 ПК-4	Л1.1 Л2.1	0	
4.3	Разработка программы псевдослучайной ге-нерации чисел. Создание модели Отладка программы Исследование программы /Лаб/	5	6	ПК-3 ПК-4	Л1.1 Л2.1	2	

	Раздел 5. Методы несанкционированного доступа к конфиденциальной информации. Каналы утечки информации ограниченного доступа						
5.1	Направления и виды разведывательной деятельности. Государственные разведывательные службы зару¬бежных стран Структура разведывательных служб частных объеди¬нений Направления и виды разведывательной деятельности /Лек/	5	2	ПК-3 ПК-4	Л1.1 Л2.1	1	
5.2	Агентурная и компьютерная разведки. Способы несанкционированного доступа к конфиденциальной информации агентурной разведки Компьютерная разведка /Ср/	5	4	ПК-4	Л1.1 Л2.1	0	
5.3	Понятие и общая классификация объектов защиты информации Понятие и общая классификация объектов защиты информации Средства и системы обработки информации как объ¬екты защиты информации Средства обеспечения объекта информатизации Помещения, в которых установлены средства обра¬ботки и помещения для конфиденциальных перего¬воров как объекты защиты информации /Лек/	5	2	ПК-3	Л1.1 Л2.1	1	
5.4	Средства и системы обработки информации как объекты защиты информации 13.1 Понятие и общая классификация объектов защиты информации Средства и системы обработки информации как объ¬екты защиты информации Средства обеспечения объекта информатизации Помещения, в которых установлены средства обра¬ботки и помещения для конфиденциальных перего¬воров как объекты защиты информации /Ср/	5	4	ПК-4	Л1.1 Л2.1	0	
5.5	Разработка программы сканирования портов. Создание модели Отладка программы Исследование программы /Лаб/	5	6	ПК-3	Л1.1 Л2.1	2	
5.6	Разработка системы ЭЦП. Создание модели Отладка программы системы Исследование системы. /Ср/	5	4	ПК-4	Л1.1 Л2.1	0	
	Раздел 6. Методы и средства и системы защиты информации						
6.1	Характеристика способов и средств по видам защиты информации. 1Виды защиты информации и сферы их действия Общие способы защиты информации Общая классификация средств защиты информации. /Лек/	5	2	ПК-4	Л1.1 Л2.1	0	

6.2	Понятие и общая структура системы защиты информации. Виды защиты информации и сферы их действия Общие способы защиты информации Общая классификация средств защиты информации Характеристика способов и средств по видам защиты информации /Ср/	5	4	ПК-3 ПК-4	Л1.1 Л2.1	1	
6.3	Компоненты комплексной системы защиты информации на предприятии и их назначение.16.1 Понятие и общая структура комплексной системы защиты информации на предприятии Компоненты комплексной системы защиты информа¬ции на предприятии и их назначение Автоматизированные системы как основной объект защиты КСЗИ /Лек/	5	2	ПК-3	Л1.1 Л2.1	1	
6.4	Разработка программы сниффера. Создание модели Отладка программы Исследование программы /Лаб/	5	6	ПК-4	Л1.1 Л2.1	2	
6.5	Разработка системы защиты от НСД. Создание модели Отладка программы системы Исследование системы. /Ср/	5	4	ОПК-7	Л1.1 Л2.1	0	
6.6	/Экзамен/	5	36	ПК-3 ПК-4	Л1.1 Л2.1 Э1 Э2	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

ВОПРОСЫ

1. Место ИБ в системе национальной безопасности;

2. Основные принципы обеспечения ИБ;

3. Классификация угроз ИБ;

4. Состав и краткая характеристика внутренних и внешних источников угроз ИБ;

5. Сущность и понятие информационной безопасности (ИБ);

6. Характеристика основных составляющих ИБ;

7. Значение ИБ для субъектов информационных отношений

8. Состав и краткая характеристика основных угроз доступности;

9. Состав и краткая характеристика основных угроз целостности;

10. Состав и краткая характеристика основных угроз конфиденциальности;

11. Классификация категорий хакеров и их целей;

12. Состав и краткая характеристика организационно-коммуникативных средств НСД;

13. Состав и краткая характеристика технических средств НСД;

14. Состав и краткая характеристика программных средств НСД;

15. Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;

16. Классификация сетевых атак;

17. Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;

18. Определение IP-спуфинга и характеристика основных средств защиты от него;

19. Определение атак типа DoS («отказ в обслуживании») и характеристика основных средств защиты от них;

20. Определение парольных атак и характеристика основных средств защиты от них;

21. Определение атак на уровне приложений и типа Man-in-the-Middle и характеристика основных средств защиты от них
22. Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;

23. Основные методы и условия неавторизованного доступа к ЛВС;

24. Краткая характеристика основных условий НСД к ЛВС;

25. Краткая характеристика основных условий раскрытия данных ЛВС;

26. Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;

27. Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;

28. Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;

29. Основные сервисы безопасности;

30. Основные принципы архитектурной безопасности и их краткая характеристика;

31. Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;

32. Основные функции централизованного управления рисками и администрирования системы безопасности;

33. Основные функции защиты управления приложениями;

34. Основные функции защиты системы сетей;

35. Основные функции защиты конечных пользователей;

36. Классификация средств защиты программного обеспечения и характеристика их основных категорий;

37. Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;

38. Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;

39. Принципы организации и технического исполнения замков защиты и защиты типа «изменение функций»;

40. Классификация средства защиты с запросом информации и характеристика их основных составляющих;

41. Назначение и принцип формирования паролей, шифров, сигнатур;

42. Назначение и основные принципы построения аппаратуры защиты;

43. Классификация средств активной защиты и характеристика их основных составляющих;

44. Определение и характеристика основных внутренних средств активной защиты;

45. Определение и характеристика основных внешних средств активной защиты;

46. Классификация средств пассивной защиты и характеристика их основных составляющих;

47. Назначение и основные принципы организации идентификации программ;

48. Назначение и основные принципы построения устройств контроля;

49. Общий состав требований по обеспечению ИБ;

50. Требования к программно□аппаратным средствам;

51. Требования к подсистеме идентификации и аутентификации;

52. Требования к подсистеме управления доступом;

53. Требования к подсистеме протоколирования аудита;

54. Требования к подсистеме защиты повторного использования объектов и к защите кри-тичной информации;

55. Требования к средствам обеспечения целостности;

56. Требования к средствам управления ИБ;

57. Общий состав требований к межсетевому экрану;

58. Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;

59. Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;

60. Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;

61. Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;
62. Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика;

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 Д. А.	Информационная безопасность открытых систем: учеб. для студентов, обучающихся по напр. "Приклад. информатика"	М.: Флинта, 2013	20

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: учеб. пособие	М.: РИО□, 2014	11

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Цифровые образовательные ресурсы: http://www.cor.home-edu.ru
Э2	едеральный центр информационно-образовательных ресурсов (ФЦИОР): http://fcior.edu.ru

6.3. Перечень программного обеспечения

6.3.1	
6.3.2	Microsoft Word,
6.3.3	MS Excel,
6.3.4	MS PowerPoint,

6.4 Перечень информационных справочных систем

6.4.1	Компьютерная справочно-правовая система «Гарант»,
6.4.2	НТЦ «Система»

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Лаборатория физики
7.2	Лаборатория управления информационной безопасностью
7.3	Лаборатория электротехники, электроники и схемотехники
7.4	Учебный серверный центр
7.5	Лаборатория технической защиты информации

7.6	Лабораторпия систем и сетей передачи информации
7.7	Лаборатория программно-аппаратных средств обеспечения информационной безопасности
7.8	Лаборатория защищенных информационных систем

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 «11» мая 2018г.
Зав.кафедрой _____ *Тищенко Е.Н.*

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Теория информационной безопасности и методология защиты информации»
(наименование дисциплины)
Направление подготовки

10.03.01 «Информационная безопасность»

Уровень образования
бакалавриат

Составитель _____ Скляров А.В., доцент, к.т.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-3 способностью администрировать подсистемы информационной безопасности объекта защиты			
З: основы администрирования подсистемы информационной безопасности объекта защиты	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
У: Пользоваться программными, программно-аппаратными средствами администрирования подсистемы информационной безопасности объекта защиты	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

В: Методами установки, настройки и обслуживания подсистемы информационной безопасности объекта защиты	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
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты			
З: Основы комплексного подхода к обеспечению информационной безопасности объекта защиты	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
У: Самостоятельно применять комплексный подход к обеспечению информационной безопасности объекта защиты	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

В: Навыками анализа эффективности политики 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

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

«Ростовский государственный экономический университет (РИНХ)»

Кафедра Информационных технологий и защиты информации
(наименование кафедры)

Вопросы к экзамену

по дисциплине «Теория информационной безопасности и методология защиты информации»
(наименование дисциплины)

1. Место ИБ в системе национальной безопасности;
2. Основные принципы обеспечения ИБ;
3. Классификация угроз ИБ;
4. Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
5. Сущность и понятие информационной безопасности (ИБ);
6. Характеристика основных составляющих ИБ;
7. Значение ИБ для субъектов информационных отношений
8. Состав и краткая характеристика основных угроз доступности;
9. Состав и краткая характеристика основных угроз целостности;
10. Состав и краткая характеристика основных угроз конфиденциальности;
11. Классификация категорий хакеров и их целей;
12. Состав и краткая характеристика организационно–коммуникативных средств НСД;
13. Состав и краткая характеристика технических средств НСД;
14. Состав и краткая характеристика программных средств НСД;
15. Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;
16. Классификация сетевых атак;
17. Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;
18. Определение IP–спуфинга и характеристика основных средств защиты от него;
19. Определение атак типа **DoS** («отказ в обслуживании») и характеристика основных средств защиты от них;
20. Определение парольных атак и характеристика основных средств защиты от них;

21.Определение атак на уровне приложений и типа **Man–in–the–Middle** и характеристика основных средств защиты от них;
22.Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;
23.Основные методы и условия неавторизованного доступа к ЛВС;
24.Краткая характеристика основных условий НСД к ЛВС;
25.Краткая характеристика основных условий раскрытия данных ЛВС;
26.Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;
27.Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;
28.Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;
29.Основные сервисы безопасности;
30.Основные принципы архитектурной безопасности и их краткая характеристика;
31.Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;
32.Основные функции централизованного управления рисками и администрирования системы безопасности;
33.Основные функции защиты управления приложениями;
34.Основные функции защиты системы сетей;
35.Основные функции защиты конечных пользователей;
36.Классификация средств защиты программного обеспечения и характеристика их основных категорий;
37.Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;
38.Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;
39. Принципы организации и технического исполнения замков защиты и защиты типа «изменение функций»;
40.Классификация средства защиты с запросом информации и характеристика их основных составляющих;
41. Назначение и принцип формирования паролей, шифров, сигнатур;
42. Назначение и основные принципы построения аппаратуры защиты;
43.Классификация средств активной защиты и характеристика их основных составляющих;
44. Определение и характеристика основных внутренних средств активной защиты;
45. Определение и характеристика основных внешних средств активной защиты;
46. Классификация средств пассивной защиты и характеристика их основных составляющих;
47. Назначение и основные принципы организации идентификации программ;

48. Назначение и основные принципы построения устройств контроля;
49. Общий состав требований по обеспечению ИБ;
50. Требования к программно–аппаратным средствам;
51. Требования к подсистеме идентификации и аутентификации;
52.Требования к подсистеме управления доступом;
53.Требования к подсистеме протоколирования аудита;
54.Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;
55.Требования к средствам обеспечения целостности;
56.Требования к средствам управления ИБ;
57.Общий состав требований к межсетевому экрану;
58.Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;
59.Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;
60.Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;
61.Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;
62.Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика;

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 Теория информационной безопасности и методология защиты информации
(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 2017 г.
Зав.кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.Б.18 «Теория информационной безопасности и методология защиты информации»

(наименование дисциплины)

Направление подготовки

10.03.01 «Информационная безопасность»

Уровень образования
бакалавриат

Составитель _____ Скляров А.В., доцент, к.т.н.
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2017

Методические указания по освоению дисциплины «Теория информационной безопасности и методология защиты информации» 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 Основы информационной безопасности, 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.