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

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основы информационной безопасности

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>)	**1 (1.1)**		**2 (1.2)**		Итого	
Недель	17,3		17,3			
Вид занятий	УП	РПД	УП	РПД	УП	РПД
Лекции	18	18	36	36	54	54
Лабораторные	36	36	36	36	72	72
В том числе инт.	18	18	18	18	36	36
Итого ауд.	54	54	72	72	126	126
Контактная	54	54	72	72	126	126
Сам. работа	18	18	72	72	90	90
Часы на контроль			36	36	36	36
Итого	72	72	180	180	252	252

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. _____ 10.05.18

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

Методическим советом направления: к.ф.-м.н., доцент, Карасев Д.Н. _____ 29.05.18

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., 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 "Основ информационной безопасности" как дисциплины профессионального цикла направлено на достижение следующих целей: развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры; развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления; привитие стремления к поиску оптимальных, простых и надежных решений; расширение кругозора.
1.2	Задачи дисциплины. Дать знания по вопросам: обеспечения информационной безопасности государства; методологии создания систем защиты информации; процессов сбора, передачи и накопления информации; методов и средств ведения информационных войн; оценки защищенности и обеспечения информационной безопасности компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.Б.16
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Для успешного освоения дисциплины студент должен иметь базовую подготовку по информатике в объеме средней школы
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Электротехника, электроника и схемотехника
2.2.2	Защита и обработка конфиденциальных документов
2.2.3	Теория информационной безопасности и методология защиты информации
2.2.4	Криптографические методы защиты информации
2.2.5	Основы управления информационной безопасностью
2.2.6	Практика по получению первичных профессиональных умений и навыков

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
Знать:
основы профессиональной деятельности в области информационной безопасности и методов защиты личности, общества и государства на базовом уровне
Уметь:
применять основы знаний в области информационной безопасности и методов защиты личности, общества и государства на базовом уровне
Владеть:
методами анализа области применения средств и методов обеспечения информационной безопасности и методов защиты личности, общества и государства на базовом уровне
ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
Знать:
основные методы реализации политики информационной безопасности на базовом уровне
Уметь:
применять основные методы реализации политики информационной безопасности на базовом уровне
Владеть:
навыками использования основных методов реализации политики информационной безопасности на базовом уровне
ПК-8: способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
Знать:
основные методы оформления рабочей технической документации на базовом уровне
Уметь:
применять действующие нормативные и методические документы на базовом уровне
Владеть:
применять основные методы оформления рабочей технической документации на базовом 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. Информационная безопасность в системе национальной безопасности Российской Федерации						
1.1	Понятие национальной безопасности: виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная,информационная, военная, пограничная, экологическая и другие /Лек/	1	2	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
1.2	Понятие национальной безопасности: лабораторные занятия по теме лекции /Лаб/	1	4	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
1.3	Понятие национальной безопасности: самостоятельная работа по теме лекции /Ср/	1	2	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
1.4	Виды защищаемой информации: основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства /Лек/	1	2	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
1.5	Виды защищаемой информации: лабораторные занятия по теме лекции /Лаб/	1	4	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
1.6	Виды защищаемой информации: самостоятельная работа по теме лекции /Ср/	1	2	ОК-5 ПК-4 ПК-8	Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
	Раздел 2. Информационная война, методы и средства ее ведения						

2.1	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение: интересы личности в информационной сфере, интересы общества в информационной сфере, интересы государства в информационной сфере; основные составляющие национальных интересов Российской Федерации в информационной сфере; угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России, угрозы информационному обеспечению государственной политики Российской Федерации, угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов, угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России; внешние источники угроз, внутренние источники угроз; направления обеспечения информационной безопасности государства; проблемы региональной информационной безопасности /Лек/	1	2	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.2	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение:практические занятия по теме лекции. /Лаб/	1	4	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.3	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение: самостоятельная работа по теме лекции /Ср/	1	2	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.4	Содержание информационного противоборства на межгосударственном уровне: информационная безопасность и информационное противоборство; субъекты информационного противоборства; цели информационного противоборства; составные части и методы информационного противоборства; информационное оружие, его классификация и возможности /Лек/	1	2	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	

2.5	Содержание информационного противоборства на межгосударственном уровне: практические занятия по теме лекции /Лаб/	1	6	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.6	Содержание информационного противоборства на межгосударственном уровне: самостоятельная работа по теме лекции /Ср/	1	2	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.7	Содержание информационного противоборства на военном уровне: методы нарушения конфиденциальности, целостности и доступности информации; причины, виды, каналы утечки и искажения информации; основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны /Лек/	1	2	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.8	Содержание информационного противоборства на военном уровне: лабораторные занятия по теме лекции /Лаб/	1	6	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.9	Содержание информационного противоборства на военном уровне: самостоятельная работа по теме лекции /Ср/	1	2	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.10	Компьюперная система как объект информационного воздействия: методы воздействия, субъекты и объекты воздействия /Лек/	1	4	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.11	Компьюперная система как объект информационного воздействия: лабораторные занятия по теме лекции /Лаб/	1	6	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.12	Компьюперная система как объект информационного воздействия: самостоятельная работа по теме лекции /Ср/	1	4	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
	Раздел 3. Критерии защищенности компьютерных систем						
3.1	Методы и средства обеспечения информационной безопасности компьютерных систем: компьютерная система как объект информационной безопасности; общая характеристика методов и средств защиты информации; организационно-правовые, технические и криптографические методы обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности /Лек/	1	4	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
3.2	Методы и средства обеспечения информационной безопасности компьютерных систем: лабораторные занятия по теме лекции /Лаб/	1	6	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
3.3	Методы и средства обеспечения информационной безопасности компьютерных систем: самостоятельная работа по теме лекции /Ср/	1	4	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	

3.4	/Зачёт/	1	0	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
3.5	Методы оценки защищенности компьютерных систем от НСД: модели, стратегии и системы обеспечения информационной безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Общие критерии /Лек/	2	4	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
3.6	Методы оценки защищенности компьютерных систем от НСД: лабораторные занятия по теме лекции /Лаб/	2	6	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	4	
3.7	Методы оценки защищенности компьютерных систем от НСД: самостоятельная работа по теме лекции /Ср/	2	14	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
	Раздел 4. Защита информации, обрабатываемой в автоматизированных системах, от технических разведок						
4.1	Классификация и возможности технических разведок: компьютерная разведка, технические каналы утечки информации при эксплуатации АС /Лек/	2	8	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
4.2	Классификация и возможности технических разведок: лабораторные занятия по теме лекции /Лаб/	2	6	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	4	
4.3	Классификация и возможности технических разведок: самостоятельная работа по теме лекции /Ср/	2	14	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
4.4	Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: классификация методов, алгоритмы оценки качества систем защиты /Лек/	2	8	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
4.5	Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: лабораторные занятия по теме лекции /Лаб/	2	8	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
4.6	Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: самостоятельная работа по теме лекции /Ср/	2	14	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
	Раздел 5. Защита АС и СВТ от внешнего электромагнитного воздействия						
5.1	Генераторы электромагнитных импульсов: эффекты, возникающие от внешнего электромагнитного воздействия на АС и СВТ /Лек/	2	8	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
5.2	Генераторы электромагнитных импульсов: лабораторные занятия по теме лекции /Лаб/	2	8	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	

5.3	Генераторы электромагнитных импульсов: самостоятельная работа по теме лекции /Ср/	2	14	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
5.4	Методы защиты АС и СВТ от внешнего электромагнитного воздействия: экранирование, создание преднамеренных помех, кодировка сигнала /Лек/	2	8	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
5.5	Методы защиты АС и СВТ от внешнего электромагнитного воздействия: лабораторные занятия по теме лекции /Лаб/	2	8	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
5.6	Методы защиты АС и СВТ от внешнего электромагнитного воздействия: самостоятельная работа по теме лекции /Ср/	2	16	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
5.7	/Экзамен/	2	36	ОК-5 ПК-4 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

ВОПРОСЫ К ЗАЧЕТУ:

1. Состав элементов внешнего периметра информационной системы
2. Состав элементов внутреннего периметра информационной системы
3. Состав угроз информационной безопасности
4. Состав каналов утечки информации
5. Какая группа каналов утечки информации используется при DDoS-атаке
6. Функции криптографии
7. Определение понятия «криптостойкость»
8. Определение понятия «криптоалгоритм» («криптосистема»)
9. Определение понятия «криптограф»
10. Определение понятия «криптоаналитик»
11. Определение понятия «криптоанализ»
12. Определение понятия «ключ криптосистемы»
13. Длина ключа в «идеальной» криптосистеме
14. Метод формирования ключа «идеальной» криптосистемы
15. Срок действия ключа в «идеальной» криптосистеме
16. Критический параметр криптосистемы
17. Смысл и ассемблерное выражение операции «замена»
18. Смысл и ассемблерное выражение операции «перестановка»
19. Смысл и ассемблерное выражение операции Шеннона
20. Соотношение операции «замена» и тактовой частоты процессора
21. Соотношение операции «перестановка» и тактовой частоты процессора
22. Алгоритм работа криптопреобразования «шифр Цезаря»
23. Основные отличия блочного и поточного шифров
24. Недостатки простого блочного алгоритма
25. Смысл и определение блочных алгоритмов с обратной связью
26. Определение операции «гаммирование»
27. Определение понятия «имитоприставка»
28. Определение понятия «однонаправленная математическая функция»
29. Достоинства и недостатки классических криптоалгоритмов
30. Достоинства и недостатки криптоалгоритмов с открытым ключем
31. Определение понятия «симметричный криптоалгоритм»
32. Определение понятия «асимметричный криптоалгоритм»
33. Количество ключей в алгоритмах классической криптографии с N абонентами
34. Количество ключей в алгоритмах open key с N абонентами
35. Определение понятия «хэш-функция»
36. Тип алгоритма и длина ключа в ГОСТ 28147-89
37. Режимы функционирования ГОСТ 28147-89
38. Сущность и назначение таблиц замен в ГОСТ 28147-89
39. Количество циклов ГОСТ 28147-89 при выработке имитоприставки
40. Количество и размер подблоков разбиения основного блока в ГОСТ 28147-89

41. Тип алгоритма и длина ключа в DES
42. Режимы функционирования DES
43. Сущность и назначение начальной и конечной перестановок в DES
44. Сущность и назначение функции расширения в DES
45. Сущность и назначение таблицы преобразований в DES
46. Типы однонаправленных функций в RSA
47. Количество ключей в RSA
48. Тип зависимости ключей в RSA
49. Исходная информация для атаки на RSA
50. Решаемая задача криптоаналитиком при атаке на RSA
51. Типы однонаправленных функций в ГОСТ Р 34.10-2001
52. Количество ключей в ГОСТ Р 34.10-2001
53. Исходная информация для атаки на ГОСТ Р 34.10-2001
54. Решаемая задача криптоаналитиком при атаке на ГОСТ Р 34.10-2001
55. Определение понятия «электронная подпись»
56. Структура электронной подписи
57. Количество ключей в алгоритмах электронной подписи
58. Используемые алгоритмы при формировании электронной подписи
59. Определение понятия «удостоверяющий центр»
60. Юридическая значимость электронной подписи

ВОПРОСЫ К ЭКЗАМЕНУ:

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.
3. Виды защищаемой информации»: основные понятия и общеметодологические принципы теории информационной безопасности.
4. Роль информационной безопасности в обеспечении национальной безопасности государства.
5. Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение»: интересы личности в информационной сфере, интересы общества в информационной сфере, интересы государства в информационной сфере.
6. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
7. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России, угрозы информационному обеспечению государственной политики Российской Федерации, угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов, угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
8. Внешние источники угроз, внутренние источники угроз; направления обеспечения информационной безопасности государства; проблемы региональной информационной безопасности.
9. Содержание информационного противоборства на межгосударственном уровне»: информационная безопасность и информационное противоборство.
10. Субъекты информационного противоборства; цели информационного противоборства; составные части и методы информационного противоборства.
11. Информационное оружие, его классификация и возможности.
12. Содержание информационного противоборства на военном уровне»: методы нарушения конфиденциальности, целостности и доступности информации.
13. Причины, виды, каналы утечки и искажения информации.
14. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
15. Компьютерная система как объект информационного воздействия»: методы воздействия, субъекты и объекты воздействия.
16. Методы и средства обеспечения информационной безопасности компьютерных систем»: компьютерная система как объект информационной безопасности.
17. Общая характеристика методов и средств защиты информации.
18. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.
19. Программно-аппаратные средства обеспечения информационной безопасности.
20. Методы оценки защищенности компьютерных систем от НСД»: модели, стратегии и системы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
22. Классификация и возможности технических разведок»: компьютерная разведка, технические каналы утечки информации при эксплуатации АС.
23. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок»: классификация методов, алгоритмы оценки качества систем защиты.
24. Анализ наиболее актуальных источников угроз со стороны технических разведок.
25. Генераторы электромагнитных импульсов: эффекты, возникающие от внешнего электромагнитного воздействия на АС

и СВТ. 26. Методы защиты АС и СВТ от внешнего электромагнитного воздействия: экранирование, создание преднамеренных помех, кодировка сигнала. 27. Методы измерения и обнаружения электромагнитных импульсов.
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	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: учеб. пособие	М.: РИО♦, 2014	11
Л1.2	Сычев Ю. Н.	Основы информационной безопасности: учебно-практическое пособие	Москва: Евразийский открытый институт, 2010	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
Л2.2	Загинайлов Ю. Н.	Основы информационной безопасности: курс визуальных лекций	Москва|Берлин: Директ-Медиа, 2015	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
Л3.2	Нестеров С. А.	Основы информационной безопасности: учебное пособие	Санкт-Петербург: Издательство Политехнического университета, 2014	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей

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

Б1.Б.16.1 «Основы информационной безопасности»
(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
ОК-5 – способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики			
З: основы профессиональной деятельности в области информационной безопасности и методов защиты личности, общества и государства	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 основы знаний в области информационной безопасности и методов защиты личности, общества и государства	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: методами анализа области применения средств и методов обеспечения информационной безопасности и методов защиты личности, общества и государства	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-4 – способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты			
З: основные методы реализации 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, Т - тест
У: применять основные методы реализации 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 , Т - тест

В: навыками использования основных методов реализации 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, Т - тест
ПК-8 – способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов			
З: основные методы оформления рабочей технической документации	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 действующие нормативные и методические документы	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 оформления рабочей технической документации	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 «Основы информационная безопасности»
(наименование дисциплины)

1.Понятие национальной безопасности.
2.Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.
3.Виды защищаемой информации»: основные понятия и общеметодологические принципы теории информационной безопасности.
4.Роль информационной безопасности в обеспечении национальной безопасности государства.
5. Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение»: интересы личности в информационной сфере, интересы общества в информационной сфере, интересы государства в информационной сфере.
6. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
7. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России, угрозы информационному обеспечению государственной политики Российской Федерации, угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов, угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
8. Внешние источники угроз, внутренние источники угроз; направления обеспечения информационной безопасности государства; проблемы региональной информационной безопасности.
9. Содержание информационного противоборства на межгосударственном уровне»: информационная безопасность и информационное противоборство.
10. Субъекты информационного противоборства; цели информационного противоборства; составные части и методы информационного противоборства.

11. Информационное оружие, его классификация и возможности.
12. Содержание информационного противоборства на военном уровне»: методы нарушения конфиденциальности, целостности и доступности информации.
13. Причины, виды, каналы утечки и искажения информации.
14. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
15. Компьютерная система как объект информационного воздействия»: методы воздействия, субъекты и объекты воздействия.
16. Методы и средства обеспечения информационной безопасности компьютерных систем»: компьютерная система как объект информационной безопасности.
17. Общая характеристика методов и средств защиты информации.
18. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.
19. Программно-аппаратные средства обеспечения информационной безопасности.
20. Методы оценки защищенности компьютерных систем от НСД»: модели, стратегии и системы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
22. Классификация и возможности технических разведок»: компьютерная разведка, технические каналы утечки информации при эксплуатации АС.
23. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок»: классификация методов, алгоритмы оценки качества систем защиты.
24. Анализ наиболее актуальных источников угроз со стороны технических разведок.
25. Генераторы электромагнитных импульсов: эффекты, возникающие от внешнего электромагнитного воздействия на АС и СВТ.
26. Методы защиты АС и СВТ от внешнего электромагнитного воздействия: экранирование, создание преднамеренных помех, кодировка сигнала.
27. Методы измерения и обнаружения электромагнитных импульсов.

«Ростовский государственный экономический университет (РИНХ)»

Кафедра Информационных технологий и защиты информации
(наименование кафедры)

Вопросы к зачету

по дисциплине «Основы информационной безопасности»
(наименование дисциплины)

1. Состав элементов внешнего периметра информационной системы
2. Состав элементов внутреннего периметра информационной системы
3. Состав угроз информационной безопасности
4. Состав каналов утечки информации
5. Какая группа каналов утечки информации используется при DDoS-атаке
6. Функции криптографии
7. Определение понятия «криптостойкость»
8. Определение понятия «криптоалгоритм» («криптосистема»)
9. Определение понятия «криптограф»
10. Определение понятия «криптоаналитик»
11. Определение понятия «криптоанализ»
12. Определение понятия «ключ криптосистемы»
13. Длина ключа в «идеальной» криптосистеме
14. Метод формирования ключа «идеальной» криптосистемы
15. Срок действия ключа в «идеальной» криптосистеме
16. Критический параметр криптосистемы
17. Смысл и ассемблерное выражение операции «замена»
18. Смысл и ассемблерное выражение операции «перестановка»
19. Смысл и ассемблерное выражение операции Шеннона
20. Соотношение операции «замена» и тактовой частоты процессора
21. Соотношение операции «перестановка» и тактовой частоты процессора
22. Алгоритм работа криптопреобразования «шифр Цезаря»
23. Основные отличия блочного и поточного шифров
24. Недостатки простого блочного алгоритма
25. Смысл и определение блочных алгоритмов с обратной связью
26. Определение операции «гаммирование»
27. Определение понятия «имитоприставка»
28. Определение понятия «однонаправленная математическая функция»
29. Достоинства и недостатки классических криптоалгоритмов
30. Достоинства и недостатки криптоалгоритмов с открытым ключем
31. Определение понятия «симметричный криптоалгоритм»
32. Определение понятия «асимметричный криптоалгоритм»
33. Количество ключей в алгоритмах классической криптографии с N абонентами
34. Количество ключей в алгоритмах open key с N абонентами
35. Определение понятия «хэш-функция»
36. Тип алгоритма и длина ключа в ГОСТ 28147-89
37. Режимы функционирования ГОСТ 28147-89
38. Сущность и назначение таблиц замен в ГОСТ 28147-89
39. Количество циклов ГОСТ 28147-89 при выработке имитоприставки

40. Количество и размер подблоков разбиения основного блока в ГОСТ 28147-89
41. Тип алгоритма и длина ключа в DES
42. Режимы функционирования DES
43. Сущность и назначение начальной и конечной перестановок в DES
44. Сущность и назначение функции расширения в DES
45. Сущность и назначение таблицы преобразований в DES
46. Типы однонаправленных функций в RSA
47. Количество ключей в RSA
48. Тип зависимости ключей в RSA
49. Исходная информация для атаки на RSA
50. Решаемая задача криптоаналитиком при атаке на RSA
51. Типы однонаправленных функций в ГОСТ Р 34.10-2001
52. Количество ключей в ГОСТ Р 34.10-2001
53. Исходная информация для атаки на ГОСТ Р 34.10-2001
54. Решаемая задача криптоаналитиком при атаке на ГОСТ Р 34.10-2001
55. Определение понятия «электронная подпись»
56. Структура электронной подписи
57. Количество ключей в алгоритмах электронной подписи
58. Используемые алгоритмы при формировании электронной подписи
59. Определение понятия «удостоверяющий центр»
60. Юридическая значимость электронной подписи

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».

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 контрольным письменным опросам

по дисциплине «Основы информационной безопасности»
(наименование дисциплины)

Модуль 1. «Информационная безопасность в системе национальной безопасности Российской Федерации»

КО 1. (Контрольный письменный опрос №1)

Вопросы для контрольного письменного опроса

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.
3. Виды защищаемой информации»: основные понятия и общеметодологические принципы теории информационной безопасности.
4. Роль информационной безопасности в обеспечении национальной безопасности государства.

Критерии оценивания:
- оценка «зачтено» выставляется, если ответы даны на все вопросы
- оценка «не зачтено» выставляется, если ответы не даны на все вопросы

Модуль 2. «Информационная война, методы и средства ее ведения»

КО 2. (Контрольный письменный опрос №2)

Вопросы для контрольного письменного опроса

1. Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение»: интересы лич-

ности в информационной сфере, интересы общества в информационной сфере, интересы государства в информационной сфере.
2. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
3. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России, угрозы информационному обеспечению государственной политики Российской Федерации, угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов, угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
4. Внешние источники угроз, внутренние источники угроз; направления обеспечения информационной безопасности государства; проблемы региональной информационной безопасности.
5. Содержание информационного противоборства на межгосударственном уровне»: информационная безопасность и информационное противоборство.
6. Субъекты информационного противоборства; цели информационного противоборства; составные части и методы информационного противоборства.
7. Информационное оружие, его классификация и возможности.
8. Содержание информационного противоборства на военном уровне»: методы нарушения конфиденциальности, целостности и доступности информации.
9. Причины, виды, каналы утечки и искажения информации.
10. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
11. Компьютерная система как объект информационного воздействия»: методы воздействия, субъекты и объекты воздействия.

Критерии оценивания:
- оценка «зачтено» выставляется, если ответы даны на все вопросы
- оценка «не зачтено» выставляется, если ответы не даны на все вопросы

Модуль 3. «Критерии защищенности компьютерных систем»

КО 3. (Контрольный письменный опрос №3)

Вопросы для контрольного письменного опроса

1. Методы и средства обеспечения информационной безопасности компьютерных систем»: компьютерная система как объект информационной безопасности.
2. Общая характеристика методов и средств защиты информации.
3. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.
4. Программно-аппаратные средства обеспечения информационной безопасности.
5. Методы оценки защищенности компьютерных систем от НСД»: модели, стратегии и системы обеспечения информационной безопасности.
6. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Критерии оценивания:
- оценка «зачтено» выставляется, если ответы даны на все вопросы
- оценка «не зачтено» выставляется, если ответы не даны на все вопросы

Модуль 4. «Защита информации, обрабатываемой в автоматизированных системах, от технических разведок»

КО 4. (Контрольный письменный опрос №4)

Вопросы для контрольного письменного опроса

1. Классификация и возможности технических разведок»: компьютерная разведка, технические каналы утечки информации при эксплуатации АС.
2. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок»: классификация методов, алгоритмы оценки качества систем защиты.
4. Анализ наиболее актуальных источников угроз со стороны технических разведок.

Критерии оценивания:
- оценка «зачтено» выставляется, если ответы даны на все вопросы
- оценка «не зачтено» выставляется, если ответы не даны на все вопросы

Модуль 5. «Информационная безопасность в системе национальной безопасности Российской Федерации»

КО 5. (Контрольный письменный опрос №5)

Вопросы для контрольного письменного опроса

1.Генераторы электромагнитных импульсов: эффекты, возникающие от внешнего электромагнитного воздействия на АС и СВТ.
2.Методы защиты АС и СВТ от внешнего электромагнитного воздействия: экранирование, создание преднамеренных помех, кодировка сигнала.
3.Методы измерения и обнаружения электромагнитных импульсов.

Критерии оценивания:
-оценка «зачтено» выставляется, если ответы даны на все вопросы
- оценка «не зачтено» выставляется, если ответы не даны на все 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 Основы информационной безопасности
(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

Б1.Б.16.1 «Основы информационной безопасности»
(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 «Основы информационной безопасности» 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.