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

Программно-аппаратная реализация алгоритмов контроля и управления

по профессионально-образовательной программе направление 09.03.04 "Программная инженерия"

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)		7 (4.1)		Итого	
Недель	18		18			
Вид занятий	УП	РПД	УП	РПД	УП	РПД
Лекции	18	18	18	18	36	36
Лабораторные	36	36	36	36	72	72
В том числе инт.	36	36	36	36	72	72
Итого ауд.	54	54	54	54	108	108
Контактная	54	54	54	54	108	108
Сам. работа	54	54	90	90	144	144
Часы на контроль			36	36	36	36
Итого	108	108	180	180	288	288

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.03.04 Программная инженененрия (уровень бакалавриата) (приказ Минобрнауки России от 12.03.2015г. №229)

Рабочая программа составлена по профессионально-образовательной программе направление 09.03.04 "Программная инженерия"

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

Программу составил(и): д.э.н., зав. кафедрой, Радченко Ю.В. _____ 11.05.18

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

Методическим советом направления: к.ф.-м.н., доцент, Карасев Д.Н. _____ 11.05.18

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, Радченко Ю.В. _____

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, Радченко Ю.В. _____

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, Радченко Ю.В. _____

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, Радченко Ю.В. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цели дисциплины. Изучение дисциплины 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.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	Методы отказоустойчивого программирования
2.1.3	Методы разработки защищенных систем
2.1.4	Программирование игровых алгоритмов
2.1.5	Проектирование и конструирование программного обеспечения
2.1.6	Теория систем и системный анализ
2.1.7	Инструменты и методы программной инженерии
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Правовая защита интеллектуальной собственности
2.2.2	Технологии системного программного обеспечения
2.2.3	Управление программными проектами
2.2.4	Архитектура вычислительных систем
2.2.5	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
2.2.6	Интегрированные CASE-средства
2.2.7	Научно-исследовательская работа
2.2.8	Подготовка к сдаче и сдача государственного экзамена
2.2.9	Преддипломная
2.2.10	Реинжиниринг систем программирования

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ПК-12: способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования
Знать:
методы пользования способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования
Уметь:
пользоваться способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования
Владеть:
способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования
ПК-19: владением навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения
Знать:
методы пользования владением навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения
Уметь:
пользоваться владением навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения
Владеть:
навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения

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/	6	2	ПК-12 ПК-19	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/	6	4	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	4	
1.3	Понятие национальной безопасности: самостоятельная работа по теме лекции /Ср/	6	2	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
1.4	Виды защищаемой информации: лабораторные занятия по теме лекции /Лаб/	6	4	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
1.5	Виды защищаемой информации: самостоятельная работа по теме лекции /Ср/	6	2	ПК-12 ПК-19	Л1.1 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/	6	2	ПК-12 ПК-19	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/	6	4	ПК-12 ПК-19	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/	6	2	ПК-12 ПК-19	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/	6	2	ПК-12 ПК-19	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/	6	4	ПК-12 ПК-19	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/	6	2	ПК-12 ПК-19	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/	6	2	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.8	Содержание информационного противоборства на военном уровне: лабораторные занятия по теме лекции /Лаб/	6	6	ПК-12 ПК-19	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/	6	12	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.10	Компьюперная система как объект информационного воздействия: лабораторные занятия по теме лекции /Лаб/	6	2	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.11	Компьюперная система как объект информационного воздействия: самостоятельная работа по теме лекции /Ср/	6	10	ПК-12 ПК-19	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/	6	4	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	4	
3.2	Методы и средства обеспечения информационной безопасности компьютерных систем: лабораторные занятия по теме лекции /Лаб/	6	6	ПК-12 ПК-19	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/	6	10	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	

3.4	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/	6	6	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	6	
3.5	Методы оценки защищенности компьютерных систем от НСД: лабораторные занятия по теме лекции /Лаб/	6	6	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
3.6	Методы оценки защищенности компьютерных систем от НСД: самостоятельная работа по теме лекции /Ср/	6	14	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
3.7	/Зачёт/	6	0	ПК-12 ПК-19	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/	7	6	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	6	
4.2	Классификация и возможности технических разведок: лабораторные занятия по теме лекции /Лаб/	7	6	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	6	
4.3	Классификация и возможности технических разведок: самостоятельная работа по теме лекции /Ср/	7	24	ПК-12 ПК-19	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: лабораторные занятия по теме лекции /Лаб/	7	8	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	6	
4.5	Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: самостоятельная работа по теме лекции /Ср/	7	24	ПК-12 ПК-19	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/	7	6	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	6	
5.2	Генераторы электромагнитных импульсов: лабораторные занятия по теме лекции /Лаб/	7	10	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	6	
5.3	Генераторы электромагнитных импульсов: самостоятельная работа по теме лекции /Ср/	7	24	ПК-12 ПК-19	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/	7	6	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	6	
5.5	Методы защиты АС и СВТ от внешнего электромагнитного воздействия: лабораторные занятия по теме лекции /Лаб/	7	12	ПК-12 ПК-19	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/	7	18	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
5.7	/Экзамен/	7	36	ПК-12 ПК-19	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	Сычев Ю. Н.	Основы информационной безопасности: учебно-практическое пособие	Москва: Евразийский открытый институт, 2010	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л1.2		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
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

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

Программно-аппаратная реализация алгоритмов контроля и управления

по профессионально-образовательной программе направление 09.03.04 "Программная инженерия"

Квалификация

Бакалавр

Ростов-на-Дону
2018 г.

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по курсам

Курс	4		5		Итого	
Вид занятий	УП	РПД	УП	РПД		
Лекции	4	4	8	8	12	12
Лабораторные	8	8	10	10	18	18
В том числе инт.	6	6	6	6	12	12
Итого ауд.	12	12	18	18	30	30
Контактная	12	12	18	18	30	30
Сам. работа	92	92	153	153	245	245
Часы на контроль	4	4	9	9	13	13
Итого	108	108	180	180	288	288

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.03.04 Программная инженененрия (уровень бакалавриата) (приказ Минобрнауки России от 12.03.2015г. №229)

Рабочая программа составлена по профессионально-образовательной программе направление 09.03.04 "Программная инженерия"

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

Программу составил(и): _____ Радченко В.В. 11.05.18

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

Методическим советом направления: _____ 11.05.18

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): _____

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): _____

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): _____

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): _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цели дисциплины. Изучение дисциплины 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.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	Методы отказоустойчивого программирования
2.1.3	Методы разработки защищенных систем
2.1.4	Программирование игровых алгоритмов
2.1.5	Проектирование и конструирование программного обеспечения
2.1.6	Теория систем и системный анализ
2.1.7	Инструменты и методы программной инженерии
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Правовая защита интеллектуальной собственности
2.2.2	Технологии системного программного обеспечения
2.2.3	Управление программными проектами
2.2.4	Архитектура вычислительных систем
2.2.5	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
2.2.6	Интегрированные CASE-средства
2.2.7	Научно-исследовательская работа
2.2.8	Подготовка к сдаче и сдача государственного экзамена
2.2.9	Преддипломная
2.2.10	Реинжиниринг систем программирования

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ПК-12: способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования
Знать:
методы пользования способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования
Уметь:
пользоваться способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования
Владеть:
способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования
ПК-19: владением навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения
Знать:
методы пользования владением навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения
Уметь:
пользоваться владением навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения
Владеть:
навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения

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/	4	2	ПК-12 ПК-19	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
1.2	Понятие национальной безопасности: самостоятельная работа по теме лекции /Ср/	4	2	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
1.3	Виды защищаемой информации: самостоятельная работа по теме лекции /Ср/	4	2	ПК-12 ПК-19	Л1.1 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:практические занятия по теме лекции. /Лаб/	4	2	ПК-12 ПК-19	Л1.1 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: самостоятельная работа по теме лекции /Ср/	4	8	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.3	Содержание информационного противоборства на межгосударственном уровне: самостоятельная работа по теме лекции /Ср/	4	8	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.4	Содержание информационного противоборства на военном уровне: самостоятельная работа по теме лекции /Ср/	4	30	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.5	Компьюперная система как объект информационного воздействия: самостоятельная работа по теме лекции /Ср/	4	32	ПК-12 ПК-19	Л1.1 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/	4	2	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
3.2	Методы и средства обеспечения информационной безопасности компьютерных систем: лабораторные занятия по теме лекции /Лаб/	4	6	ПК-12 ПК-19	Л1.1 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/	4	10	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
3.4	/Зачёт/	4	4	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
3.5	Методы оценки защищенности компьютерных систем от НСД: лабораторные занятия по теме лекции /Лаб/	5	6	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
3.6	Методы оценки защищенности компьютерных систем от НСД: самостоятельная работа по теме лекции /Ср/	5	24	ПК-12 ПК-19	Л1.1 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/	5	4	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
4.2	Классификация и возможности технических разведок: лабораторные занятия по теме лекции /Лаб/	5	2	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
4.3	Классификация и возможности технических разведок: самостоятельная работа по теме лекции /Ср/	5	23	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
4.4	Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: самостоятельная работа по теме лекции /Ср/	5	44	ПК-12 ПК-19	Л1.1 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/	5	2	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	

5.2	Генераторы электромагнитных импульсов: лабораторные занятия по теме лекции /Лаб/	5	2	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
5.3	Генераторы электромагнитных импульсов: самостоятельная работа по теме лекции /Ср/	5	24	ПК-12 ПК-19	Л1.1 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/	5	2	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
5.5	Методы защиты АС и СВТ от внешнего электромагнитного воздействия: самостоятельная работа по теме лекции /Ср/	5	28	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
5.6	Контрольная работа. Перечень заданий для контрольной работы представлен в Приложении 1 к рабочей программе дисциплины. /Ср/	5	10	ПК-12 ПК-19	Л1.1 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
5.7	/Экзамен/	5	9	ПК-12 ПК-19	Л1.1 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	Сычев Ю. Н.	Основы информационной безопасности: учебно-практическое пособие	Москва: Евразийский открытый институт, 2010	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л1.2		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
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 Информационные
технологии и защита информации
Протокол № 10 от 11.05. 2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Программно-аппаратная реализация алгоритмов контроля и управления

Направление подготовки
09.03.04 «Программная инженерия»

Уровень образования
Бакалавриат

Составитель _____ Радченко Ю.В. доцент к.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

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-12 способность к формализации в своей предметной области с учетом ограничений используемых методов исследования			
З. -методы пользования способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования	Семейство ОС Windows. Этапы установки Windows. Аппаратные требования Windows.	полнота и содержательность ответа умение приводить примеры	О
У. -пользоваться способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования	RAID. Аппаратный и программный. Типы. RAID в Windows. Работа с дисками в Windows.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР,
В. способностью к формализации в своей предметной области с учетом ограничений используемых методов исследования	Аппаратные устройства для разграничения доступа в сети.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР,
ПК-19 владением навыками моделирования, анализа и использование формальных методов конструирования программного обеспечения			
З. методы пользования владением навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения	поиск и сбор необходимой литературы	полнота и содержательность ответа умение приводить примеры	О
У. пользоваться владением навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения	проведение моделирования	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР,
В. навыками	Методами	полнота и	О, ЛР,

моделирования, анализа и использования формальных методов конструирования программного обеспечения	конструирования программного обеспечения	содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	

О – опрос, ЛР- лабораторная работа,

3.2 Шкалы оценивания:

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

84-100 баллов (оценка «отлично»)
67-83 баллов (оценка «хорошо»)
50-66 баллов (оценка «удовлетворительно»)
0-49 баллов (оценка «неудовлетворительно»)

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

В разделе приводятся типовые варианты оценочных средств: вопросы к экзамену, задания для опроса, лабораторные работы, тематика курсовых проектов, экзаменационный билет.

ВОПРОСЫ К ЗАЧЕТУ по дисциплине **Программно-аппаратная реализация алгоритмов контроля и управления**

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:

-50-100 баллов («зачет») – 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; 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; 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 («незачет») – 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

Вопросы к экзамену
по дисциплине Программно-аппаратная реализация алгоритмов контроля и управления

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.

Критерии оценивания:
- 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.

Задания для опроса
по дисциплине Программно-аппаратная реализация алгоритмов контроля и управления

Вариант 1
Семейство ОС Windows.
Этапы установки Windows.
Аппаратные требования Windows.

Вариант 2
RAID. Аппаратный и программный. Типы.
RAID в Windows.
Работа с дисками в Windows.

Вариант 3
Источники резервного питания
Резервное копирование данных.
Аппаратные устройства для разграничения доступа в сети.

Вариант 4
Служба каталогов Windows.
Домен, дерево, лес в службе каталогов Windows.
Выбор аппаратных компонентов для организации серверных центров.

Вариант 5
Служба каталогов Active Directory.
Установка и настройка AD.
Управление пользователями с помощью AD.

Вариант 6

Группы в AD. Типы групп.
Разграничение доступа к ресурсам.
Система безопасности Windows.

Вариант 7
Политика безопасности, наследование политики безопасности
Протокол безопасности Kerberos.
Firewall: назначение, принцип работы.

Вариант 8
Microsoft ISA Server: особенности установки и настройки.
Виды адресаций в TCP/IP сетях
IP адрес: назначение, структура, применение

Вариант 9
DNS имя: назначение, структура, применение
Семиуровневая модель OSI.
Характеристика стэка протоколов TCP/IP.

Вариант 10
Виды адресации в IP сетях.
Протокол IP: назначение, структура заголовка, принципы работы
Протокол TCP: назначение, структура заголовка, основные режимы работы

Вариант 11
Маршрутизация. Таблицы маршрутизации
Службы Windows для мониторинга и оптимизации.
Мониторинг и оптимизация производительности дисков.

Вариант 12
Работа с дисковыми квотами.
Сжатие и шифрование данных средствами ОС.
Консоль "Производительность": назначение, состав.

Вариант 13
Оснастка "Системный монитор"
Оснастка "Журналы"
Утилита "Диспетчер задач": назначение, функции.

Вариант 14
Описание протоколов VPN
Компоненты VipNet
Secret Net назначение и функции

Вариант 15
Основные особенности использования Secret Net
Сравнительная характеристика Proxy и Nat серверов
Протокол безопасности IpSec

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

Кафедра Информационные технологии и защита информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

по дисциплине Программно-аппаратная реализация алгоритмов контроля и управления

1) Семейство ОС Windows.
2) Группы в AD. Типы групп.
3) Маршрутизация. Таблицы маршрутизации

Составитель _____ Радченко Ю.В.

Заведующий кафедрой ИТ и ЗИ_____ Тищенко Е.Н.

«____» _____ 20____ г.

Критерии оценивания:

- 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.

Лабораторные работы
по дисциплине Программно-аппаратная реализация алгоритмов контроля и управления

Лабораторная работа №1

Запуск менеджера виртуальных машин. Установка виртуальных машин: MS Windows Server, MS Windows 7. Настройка одноранговой сети. Создание учетных записей пользователей. Настройка локальных политик паролей.

Создание иерархической структуры сети. Установка контроллера домена. Управление учетными записями пользователей.

Лабораторная работа №2

Ознакомление с аппаратными комплексами защиты от несанкционированного доступа к ИС. Программно-аппаратный комплекс «Соболь»: ознакомление, установка, настройка. Аппаратные средства биометрической идентификации.

Лабораторная работа №3

Создание на виртуальном сервере сетевого ресурса. Настройка доступа к созданному ресурсу в одноранговой и иерархической сети. Виды доступа. Наследование прав на сетевые ресурсы. Использование групп безопасности для организации доступа к сетевым рессурсам.

Лабораторная работа №4

Установка в виртуальную сетевую среду на сервер межсетевого экрана. Первичная настройка межсетевого экрана. Формирование правил фильтрации пакетов. Проверка уровня защищенности требованиям.

Лабораторная работа №5

Установка в виртуальной среде антивирусного комплекса. Настройка основных параметров. Сканирование дисков и объектов.

Лабораторная работа №6

Работа с программным RAID в Windows сервер. Создание дополнительного виртуального жесткого диска. Подключение диска к виртуальному серверу. Создание RAID–массива. Генерация события отказа и оценка работоспособности RAID-массива.

Лабораторная работа №7

Установка и настройка утилиты «Сетевой монитор». Оценка сетевого трафика. Сбор трафика. Анализ трафика. Определение принадлежности пакета. Перехват передаваемых данных.

Лабораторная работа №8

Разворачивание архитектуры VPN с использованием стандартных средств защиты Windows сервер.

2. Методические рекомендации по выполнению лабораторных работ

Лабораторные работы выполняются с учетом приобретенных знаний по предшествующим дисциплинам, теоретического материала дисциплины, с помощью и консультациями (при необходимости) преподавателя на занятиях.

3. Критерии оценки:

- 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.

4. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

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 устном виде. Количество вопросов в экзаменационном задании – 3. 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 Информационные технологии и
защита информации
Протокол №10 от 11.05.18 г.
Зав.кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Программно-аппаратная реализация алгоритмов контроля и управления

Направление подготовки

09.03.04 «Программная инженерия»

Уровень образования

Бакалавриат

Составитель _____ Радченко Ю.В. доцент к.э.н.
(подпись) Ф.И.О., должность, ученая степень, ученое звание

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Программно-аппаратная реализация алгоритмов контроля и управления» адресованы студентам всех форм обучения.

Учебным планом по направлению подготовки 09.03.04 «Программная инженерия» предусмотрены следующие виды занятий:

лекционные

лабораторные

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

При подготовке к лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме;

– письменно решить домашнее задание, рекомендованные преподавателем при изучении каждой темы.

По согласованию с преподавателем студент может подготовить реферат, доклад или сообщение по теме занятия. В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

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

Студент должен готовиться к предстоящим лабораторным занятиям по всем, обозначенным в рабочей программе дисциплины вопросам.

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

- интерактивная доска для подготовки и проведения лекционных занятий;

- размещение материалов курса в системе дистанционного обучения http://do.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.