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 2018 г.

Рабочая программа дисциплины

Специальные методы исследования аппаратных средств информационных систем

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>)	7 (4.1)		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Практические	54	54	54	54
В том числе инт.	6	6	6	6
Итого ауд.	54	54	54	54
Контактная	54	54	54	54
Сам. работа	18	18	18	18
Итого	72	72	72	72

ОСНОВАНИЕ

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

Рабочая программа составлена

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

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

Программу составил(и): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____ 11.05.18

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

Методическим советом направления *к.ф.-м.н., декан, Карасёв Д.Н.* _____ 16.05.18

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)*к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

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): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

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): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

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): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цели освоения дисциплины: обучение практическим методам организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации. и практическим навыкам работы с нормативно-правовой базой.
1.2	Задачи освоения дисциплины: ознакомление с техническими каналами утечки информации; изучение способов и средств защиты информации, обрабатываемой техническими средствами; изучение способов и средств защиты выделенных (защищаемых) помещений от утечки информации; изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам; обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях; обучение основам правового регулирования отношений в информационной сфере, основы правового регулирования отношений в области интеллектуальной собственности и способам защиты этой собственности; формирование навыков по поиску необходимых нормативных правовых актов и работе с нормативными и распорядительными документами

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	ФТД.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Необходимыми условиями для успешного освоения дисциплины являются навыки, знания и умения, полученные в результате изучения дисциплин:
2.1.2	Методы и средства обеспечения информационной безопасности
2.1.3	Защита информационных процессов и систем
2.1.4	Защита от удаленных сетевых атак
2.1.5	Аппаратные средства вычислительной техники
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Комплексное обеспечение защиты информации объекта информатизации
2.2.2	Методы и средства обеспечения информационной безопасности

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

Знать:

общие характеристики процессов сбора, передачи, обработки и накопления информации, технических средств реализации информационных процессов; состав и структуру информационных процессов; нормативные методические документы ФСБ России, ФСТЭК России данной области; принципы работы, связанные с обеспечением комплексной защиты информации на основе существующих программ и методик; основные направления применения криптографических технологий при защите АС

Уметь:

применять аппаратные средства для проведения контроля степени защищенности по различным каналам утечки информации; использовать стандартные алгоритмы криптографической защиты

Владеть:

владеть терминологией в области систем обработки, хранения и передачи информации; действующими нормативными и методическими документами

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Знать:

методы и средства контроля эффективности защиты информации от утечки по техническим каналам

Уметь:

применять аппаратные средства для проведения контроля степени защищенности по различным каналам утечки информации

Владеть:

навыками поиска необходимых нормативных правовых актов и работой с нормативными и распорядительными документами

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Интре ракт.	Примечание

	Раздел 1. Аттестация и Государственное лицензирование деятельности в области защиты информации						
1.1	Тема "Государственное лицензирование деятельности в области ЗИ" Аттестация программных ресурсов по требованиям информационной безопасности /Пр/	7	6	ПК-1 ПК-6	Л1.1 Л2.8 Э1 Э3 Э4 Э5	0	
1.2	Тема "Государственное лицензирование деятельности в области ЗИ" Государственное лицензирование деятельности в области защиты информации /Пр/	7	2	ПК-6	Л1.2 Л2.7 Л2.8 Э1 Э3 Э4 Э5	0	
1.3	Тема "Государственное лицензирование деятельности в области ЗИ" Подготовка рабочей документации для организации лицензирования организации в области защиты информации. /Пр/	7	4	ПК-6	Л1.1 Э3 Э4 Э5	2	
1.4	Тема "Государственное лицензирование деятельности в области ЗИ" Проведение сертификационных испытаний, реализация, монтаж, наладка, установка и ремонт шифровальных средств, предназначенных для криптографической защиты информации при ее обработке, хранении и передаче по каналам связи, а также предоставление услуг по шифрованию информации. /Пр/	7	4	ПК-1 ПК-6	Л1.2 Л2.1 Л2.2 Л2.5 Э3 Э4 Э5	0	
1.5	Тема "Государственное лицензирование деятельности в области ЗИ" Программа информационной безопасности России и пути ее реализации /Ср/	7	4	ПК-6	Л1.2 Э2 Э3 Э4 Э5	0	
1.6	Тема "Государственное лицензирование деятельности в области ЗИ" Правовое обеспечение защиты государственной тайны Правовая защита конфиденциальной информации Нормативно-правовое регулирование профессиональной тайны Нормативно-правовое регулирование служебной тайны Правовое регулирование отношений по защите КТ на предпри-ятии Защита коммерческой информации в договорной документации /Ср/	7	6	ПК-6	Л1.2 Л2.4 Л2.8 Э1 Э4	0	
	Раздел 2. Специальные проверки и специальные исследования						
2.1	Тема "Специальные проверки и специальные исследования" Порядок проведения специальной проверки технических средств /Пр/	7	2	ПК-1 ПК-6	Л1.1 Э3 Э4 Э5	0	
2.2	Тема "Специальные проверки и специальные исследования" Специальная проверка технических средств /Пр/	7	4	ПК-1 ПК-6	Л1.2 Л2.1 Л2.2 Э5	2	
2.3	Тема "Специальные проверки и специальные исследования" Подготовка к проведению специальных обследований. /Пр/	7	2	ПК-1 ПК-6	Л1.1 Л1.2 Л2.2 Э3 Э4 Э5	0	

2.4	Выполнение поисковых мероприятий специальных исследований /Пр/	7	4	ПК-1 ПК-6	Л1.1 Л1.2 Л2.2 Э3 Э4 Э5	0	
2.5	Тема "Специальные проверки и специальные исследования" Специальные исследования побочных электромагнитных излучений и наводок. Основное содержание работ /Пр/	7	2	ПК-1 ПК-6	Л1.1 Л1.2 Л2.1 Л2.2 Э3 Э4 Э5	0	
2.6	Тема "Специальные проверки и специальные исследования" Специальные исследования побочных электромагнитных излучений и наводок.. Особенности специальных иссле-дований ПЭМИН /Пр/	7	4	ПК-1 ПК-6	Л1.1 Л1.2 Л2.1 Л2.2 Э3 Э4 Э5	0	
2.7	Тема "Специальные проверки и специальные исследования" Специальные исследования в области акустики и виброакустики. Основные положения методики исследований. Объекты контроля и их описание. /Пр/	7	2	ПК-1 ПК-6	Л1.1 Л1.2 Л2.1 Л2.2 Л2.6	0	
2.8	Тема "Специальные проверки и специальные исследования" Специальные исследования в области акустики и виброакустики. Средства измерения. Особенности применения системы активной защиты. /Пр/	7	4	ПК-6	Л1.1 Л1.2 Л2.1 Л2.2 Л2.6 Э3 Э4 Э5	0	
2.9	Специальные исследования в области акустоэлектрических преобразований. Основные положения методики исследований. /Пр/	7	4	ПК-6	Л1.1 Л1.2 Л2.1 Л2.2 Л2.6 Э3 Э4 Э5	0	
2.10	Тема "Специальные проверки и специальные исследования" Специальные исследования в области акустоэлектрических преобразований. Результаты специальных исследований технических средств. Средства измерения. /Пр/	7	4	ПК-1 ПК-6	Л1.1 Л1.2 Л2.1 Л2.2 Л2.6 Э3 Э4 Э5	2	
2.11	Тема "Специальные проверки и специальные исследования" ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ Правовые основы деятельности службы безопасности Правовые основы использования технических средств сбора и защиты информации /Ср/	7	6	ПК-6	Л1.1 Л2.8 Л2.9	0	
	Раздел 3. Аттестация автоматизированных систем и программных ресурсов						
3.1	Тема: "Аттестация автоматизированных систем и программных ресурсов" Аттестация АС. Классы АС и группы АС. Средства защиты информации необходимые для аттестации. /Пр/	7	2	ПК-1 ПК-6	Л1.1 Л1.2 Л2.8 Э1	0	
3.2	Тема: "Аттестация автоматизированных систем и программных ресурсов" Порядок аттестации программных ресурсов объектов информатизации /Пр/	7	4	ПК-1 ПК-6	Л1.1 Л1.2 Л2.7	0	

3.3	Тема: "Аттестация автоматизированных систем и программных ресурсов" Математические и методические средства защиты /Ср/	7	2	ПК-1 ПК-6	Л1.1 Л2.3 Л2.5	0	
3.4	/Зачёт/	7	0	ПК-1 ПК-6	Л1.1 Л1.2 Л2.1 Л2.2 Л2.4 Л2.5 Л2.8 Э1 Э3 Э4 Э5	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

Вопросы к зачёту

1. Объекты защиты с позиции организации и эффективного обеспечения КЗИ, условия размещения объектов защиты.
2. Этапы организации КЗИ (комплексной защиты информации)
3. Классификация ТКУИ (технических каналов утечки информации)
4. Оценка оперативных возможностей “нарушителя”, планирование и реализация операции по прослушиванию объекта
5. Тактические возможности злоумышленника
6. Средства выявления аппаратуры перехвата информации (анализаторы спектра, нелинейные радиолокаторы, рентгеновские установки)
7. Специальные технические средства для физического поиска (эндоскопы, досмотровые зеркала)
8. Методика планирования поисковых работ
9. Подготовка поисковой операции
10. Работа поисковой бригады на объекте (радиомониторинг, визуальный осмотр, проверка электронных приборов)
11. Работа поисковой бригады на объекте (проверка предметов интерьера и мебели, провер-ка коммуникационных изделий, обследование слаботочных линий)
12. Работа поисковой бригады на объекте (проверка ограждающих конструкций, проверка автомобиля, заключение по проведении работ)
13. Технические возможности по перехвату информации (радиомикрофоны, телефонные передатчики, диктофонные адаптеры)
14. Технические возможности по перехвату информации (проводные микрофоны, ультра-звуковые системы, направленные микрофоны)
15. Технические возможности по перехвату информации (стетоскопические датчики, лазерные микрофоны, системы для перехвата ПЭМИН)
16. Технические возможности по перехвату информации (высокочастотное навязывание, перехват остаточных сигналов в цепях питания,заземления, портативная звукозаписывающая аппаратура)
17. Цели защиты информации, органы защиты государственной тайны
18. Назначение и структура системы лицензирования деятельности в области ЗГТ
19. Государственное лицензирование деятельности в области защиты информации
20. Создание ВП, для проведения конфиденциальных переговоров
21. Аттестация выделенного помещения (ВП) - категории ВП, средства защиты информации необходимые для аттестации ВП
22. Аттестация выделенного помещения (ВП) - основные работы при проведении аттеста-ции
23. Аттестация автоматизированной системы (АС) – классы АС, средства защиты информа-ции необходимые для аттестации АС
24. Аттестация автоматизированной системы (АС) - основные работы при проведении аттестации
25. Специальные проверки - общие положения, термины и определения
26. Специальные исследования - общие положения, термины и определения
27. Российское программное обеспечение – операционная система МСВС
28. Аттестация программных ресурсов по требованиям защиты информации
29. Специальные исследования побочных электромагнитных излучений и наводок
30. Специальные исследования в области защиты речевой информации
31. Специальные исследования в области акустоэлектрических преобразований
32. Средства защиты от НСД (Secret Net 6.0) – назначение, возможности
33. Средства защиты от НСД (Страж 3.0) – назначение, возможности
34. Назначение и принцип работы прибора “вибро-шумомер “Октава 110А”
35. Назначение и принцип работы прибора “Детектор поля “ST-007”
36. Назначения и принцип работы “Электронный анализатор спектра “Agilent

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,	Заглавие	Издательство, год	Колич-во
Л1.1	Шаньгин В. Ф.	Комплексная защита информации в корпоративных системах: учеб. пособие для студентов вузов, обучающихся по напр. 230100 "Информатика и вычислит. техника"	М.: ФОРУМ, 2010	30
Л1.2	Зайцев А. П., Шелупанов А. А., Мещеряков Р. В., Голубятников И. В.	Технические средства и методы защиты информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по спец. 090102-"Компьютер. безопасность", 090105 -"Комплекс. обеспечение информ. безопасности автоматизир. систем", 090106-"Информ. безопасность телекоммуникац. систем"	М.: Горячая линия -Телеком, 2014	25

6.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Шейдаков Н. Е., Серпенинов О. В., Тищенко Е. Н.	Физические основы защиты информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. подгот. "Информ. безопасность"	М.: РИО□, 2016	110
Л2.2	Шейдаков Н. Е., Тищенко Е. Н.	Краткий курс физики для технических специальностей: учеб. пособие	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2014	63
Л2.3	Фомичев В. М.	Дискретная математика и криптология: курс лекций / biblioclub.ru/index.php?page=book_red&id=89387	, 2003	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.4	Сычев Ю. Н.	Основы информационной безопасности: учебно-практическое пособие / biblioclub.ru/index.php?page=book_red&id=90790	Москва: Евразийский открытый институт, 2010	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.5	Спицын В. Г.	Информационная безопасность вычислительной техники: учебное пособие / biblioclub.ru/index.php?page=book_red&id=208694	Томск: Эль Контент, 2011	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.6	Иванов А. В., Трушин В. А.	Защита речевой информации от утечки по акустоэлектрическим каналам: учебное пособие / biblioclub.ru/index.php?page=book_red&id=228846	Новосибирск: НГТУ, 2012	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.7	Громов Ю. Ю., Мартемьянов Ю. Ф., Букурако Ю. К., Иванова О. Г., Однолько В. Г.	Организация безопасной работы информационных систем: учебное пособие / biblioclub.ru/index.php?page=book_red&id=277794	Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.8	Лапонина О. Р.	Криптографические основы безопасности / biblioclub.ru/index.php?page=book_red&id=429092	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.9	Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В.	Аудит информационной безопасности органов исполнительной власти: учебное пособие / biblioclub.ru/index.php?page=book_red&id=93259	Москва: Издательство «Флинта», 2016	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Информационные технологии в юридической деятельности: учебное пособие Москва: ЮНИТИ-ДАНА, 2014 / https://biblioclub.ru/index.php?page=book_red&id=447909
Э2	Информационно-телекоммуникационные и компьютерные технологии, устройства и системы : состояние и перспективы развития в Южном федеральном университете: монография / под редакцией Каляева И.А., Кухаренко А.П.Ростов: Издательство Южного федерального университета, 2010 / https://biblioclub.ru/index.php?page=book_red&id=241054
Э3	Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите ФСТЭК / http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty
Э4	Перечень актов. Утвержден приказом ФСТЭК / http://fstec.ru/normotvorcheskaya/perechen-obyazatelnykh-trebovanij

Э5	Сведения о лицензионной деятельности ФСТЭК России в области технической защиты информации / http://fstec.ru/litsenzionnaya-deyatelnost/tekhnicheskaya-zashchita-informatsii
6.3. Перечень программного обеспечения	
6.3.1	Microsoft Office
6.4 Перечень информационных справочных систем	

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Специальные методы исследования аппаратных средств информационных систем»
(наименование дисциплины)

10.03.01 Информационная безопасность

10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель _____ Шейдаков Н.Е., доцент каф. ИТиЗИ, к.ф.-м.н., доцент
(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 3

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания 3

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 5

4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций 11

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-1 – способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации			
Знать: общие характеристики процессов сбора, передачи, обработки и накопления информации, технических средств реализации информационных процессов; состав и структуру информационных процессов; нормативные методические документы ФСБ России, ФСТЭК России данной области; принципы работы, связанные с обеспечением комплексной защиты информации на основе существующих программ и методик; основные направления применения криптографических технологий при защите АС	*поиск и сбор необходимой литературы, использование современных информационно- коммуникационных технологий и глобальных информационных ресурсов*	*соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры;умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации*	*О – опрос (вопрос 1), Р – реферат*
Уметь: применять аппаратные средства для проведения контроля степени за-	*решение практических задач по специальным проверкам и исследовани-*	*объем выполненных работы (в полном, не полном объеме); соответствие от-*	*О – опрос (вопрос 1), Р – реферат*

щищенности по различным каналам утечки информации; использовать стандартные алгоритмы криптографической защиты	*ям АС обработки данных; анализ результатов специальных проверок, оформление отчетных документов; моделирование лабораторных измерений спец. аппаратуры*	*чета требованиям изложенным в задании к практическим заданиям*	
Владеть владеть терминологией в области систем обработки, хранения и передачи информации; действующими нормативными и методическими документами	*решение практических задач по специальным проверкам и исследованиям АС и обработки данных; анализ результатов специальных проверок, оформление отчетных документов*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к практическим заданиям*	*О – опрос (вопрос 1),* *Р – реферат*
ПК-6 – способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации			
Знать: методы и средства контроля эффективности защиты информации от утечки по техническим каналам	*поиск и сбор необходимой литературы, использование современных информационно- коммуникационных технологий и глобальных информационных ресурсов*	*соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры;умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации*	*О – опрос (вопрос 1),* *Р – реферат*
Уметь: применять аппаратные средства для проведения контроля степени защищенности по различным каналам утечки информации	*решение практических задач по специальным проверкам и исследованиям АС обработки данных; анализ результатов специальных проверок, оформление отчетных документов; моделирование лабораторных измерений спец.*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к практическим заданиям*	*О – опрос (вопрос 1),* *Р – реферат*

	аппаратуры		
Владеть: навыками поиска необходимых нормативных правовых актов и работой с нормативными и распорядительными документами	*решение практических задач по специальным проверкам и исследованиям АС обработки данных; анализ результатов специальных проверок, оформление отчетных документов*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к практическим заданиям*	*О – опрос (вопрос 1),* *Р – реферат*

2.2 Шкалы оценивания:

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

для зачета
50-100 баллов (зачет)
0-49 баллов (незачет)

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

Модуль 1. «Аттестация и Государственное лицензирование деятельности в области защиты информации»

О 1. (письменный опрос №1)

Вопросы для контрольного письменного опроса
1. Теоретические вопросы

1.1. **Вопросы для контрольного письменного опроса**
1. Теоретические вопросы

1. Объекты защиты с позиции организации и эффективного обеспечения КЗИ, условия размещения объектов защиты.
2. Этапы организации КЗИ (комплексной защиты информации)
3. Какие документы являются нормативно-техническими при проведении аттестации объектов?
4. Что понимают под аттестацией объектов информатизации?

5. Из какого комплекса работ состоит проверка возможности утечки информации по техническим каналам?
6. Какие полномочия предоставляет действующий «Аттестат соответствия»?
7. Какие объекты подлежат обязательной аттестации?
8. Какие оценки включает в себя разведдоступность объекта информатизации?
9. Классификация ТКУИ (технических каналов утечки информации)
10. Оценка оперативных возможностей “нарушителя”, планирование и реализация операции по прослушиванию объекта
11. Тактические возможности злоумышленника
12. Методика планирования поисковых работ
13. Подготовка поисковой операции
14. Работа поисковой бригады на объекте (радиомониторинг, визуальный осмотр, проверка электронных приборов)
15. Работа поисковой бригады на объекте (проверка предметов интерьера и мебели, проверка коммуникационных изделий, обследование слаботочных линий)
16. Работа поисковой бригады на объекте (проверка ограждающих конструкций, проверка автомобиля, заключение по проведении работ)
17. Цели защиты информации, органы защиты государственной тайны
18. Назначение и структура системы лицензирования деятельности в области ЗГТ
19. Государственное лицензирование деятельности в области защиты информации

Модуль 2. Специальные проверки и специальные исследования.

О 2. (письменный опрос №2)

Вопросы для контрольного письменного опроса

1. Теоретические вопросы

1. Технические возможности по перехвату информации (радиомикрофоны, телефонные передатчики, диктофонные адаптеры)
2. Технические возможности по перехвату информации (проводные микрофоны, ультра-звуковые системы, направленные микрофоны)
3. Технические возможности по перехвату информации (стетоскопические датчики, лазерные микрофоны, системы для перехвата ПЭМИН)
4. Технические возможности по перехвату информации (высокочастотное навязывание, перехват остаточных сигналов в цепях питания, заземления, портативная звукозаписывающая аппаратура)
5. Специальные проверки - общие положения, термины и определения
6. Специальные исследования - общие положения, термины и определения

7. Специальные исследования побочных электромагнитных излучений и наводок
8. Специальные исследования в области защиты речевой информации
9. Специальные исследования в области акустоэлектрических преобразований
10. Средства защиты от НСД (Secret Net 6.0) – назначение, возможности
11. Средства защиты от НСД (Страж 3.0) – назначение, возможности
12. Назначение и принцип работы прибора "вибро-шумомер "Октава 110А"
13. Назначение и принцип работы прибора "Детектор поля "ST-007"
14. Назначения и принцип работы "Электронный анализатор спектра
15. Средства выявления аппаратуры перехвата информации (анализаторы спектра, нелинейные радиолокаторы, рентгеновские установки)
16. Специальные технические средства для физического поиска (эндоскопы, досмотровые зеркала)
17. Что представляют собой специальные проверки объекта защиты?
18. Комплекс каких мероприятий входит в специальные обследования объекта защиты?
19. Для чего производится легендирование специальных обследований выделенных помещений?
20. Из каких действий состоят поисковые мероприятия на объекте?
21. С какой целью проводятся специальные исследования?
22. Что является конечным результатом специальных исследований?
23. Какие объекты являются исследуемыми при проведении специальных исследований в области акустики?
24. На чем базируется действующая методика измерений акустических и виброакустических характеристик различных сред?
25. Что понимают под прямым акустоэлектрическим преобразованием?
26. Что понимают под модуляционным акустоэлектрическим преобразованием?
27. Демаскирующие признаки сетевых акустических закладок.
28. Демаскирующие признаки проводной микрофонной системы подслушивания.
29. Демаскирующие признаки автономных некамуфлированных акустических закладок.
30. Демаскирующие признаки сетевых акустических закладок.
31. Демаскирующие признаки полу активных акустических радиозакладок.

Модуль 3. Аттестация автоматизированных систем и программных ресурсов

О 3. (письменный опрос №3)

Вопросы для контрольного письменного опроса

1. Теоретические вопросы

1. Цели защиты информации, органы защиты государственной тайны
2. Назначение и структура системы лицензирования деятельности в области ЗГТ
3. Государственное лицензирование деятельности в области защиты информации
4. Создание ВП, для проведения конфиденциальных переговоров
5. Аттестация выделенного помещения (ВП) - категории ВП, средства защиты информации необходимые для аттестации ВП
6. Аттестация выделенного помещения (ВП) - основные работы при проведении аттестации
7. Аттестация автоматизированной системы (АС) – классы АС, средства защиты информа-ции необходимые для аттестации АС
8. Аттестация автоматизированной системы (АС) - основные работы при проведении аттестации
9. Российское программное обеспечение – операционная система МСВС
10. Аттестация программных ресурсов по требованиям защиты информации

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

по дисциплине «Специальные методы исследования аппаратных средств информационных систем»
(наименование дисциплины)

1. Объекты защиты с позиции организации и эффективного обеспечения КЗИ, условия размещения объектов защиты.
2. Этапы организации КЗИ (комплексной защиты информации)
3. Классификация ТКУИ (технических каналов утечки информации)
4. Оценка оперативных возможностей “нарушителя”, планирование и реализация операции по прослушиванию объекта
5. Тактические возможности злоумышленника

6. Средства выявления аппаратуры перехвата информации (анализаторы спектра, нелинейные радиолокаторы, рентгеновские установки)
7. Специальные технические средства для физического поиска (эндоскопы, досмотровые зеркала)
8. Методика планирования поисковых работ
9. Подготовка поисковой операции
10. Работа поисковой бригады на объекте (радиомониторинг, визуальный осмотр, проверка электронных приборов)
11. Работа поисковой бригады на объекте (проверка предметов интерьера и мебели, проверка коммуникационных изделий, обследование слаботочных линий)
12. Работа поисковой бригады на объекте (проверка ограждающих конструкций, проверка автомобиля, заключение по проведении работ)
13. Технические возможности по перехвату информации (радиомикрофоны, телефонные передатчики, диктофонные адаптеры)
14. Технические возможности по перехвату информации (проводные микрофоны, ультра-звуковые системы, направленные микрофоны)
15. Технические возможности по перехвату информации (стетоскопические датчики, лазерные микрофоны, системы для перехвата ПЭМИН)
16. Технические возможности по перехвату информации (высокочастотное навязывание, перехват остаточных сигналов в цепях питания, заземления, портативная звукозаписывающая аппаратура)
17. Цели защиты информации, органы защиты государственной тайны
18. Назначение и структура системы лицензирования деятельности в области ЗГТ
19. Государственное лицензирование деятельности в области защиты информации
20. Создание ВП, для проведения конфиденциальных переговоров
21. Аттестация выделенного помещения (ВП) - категории ВП, средства защиты информации необходимые для аттестации ВП
22. Аттестация выделенного помещения (ВП) - основные работы при проведении аттестации
23. Аттестация автоматизированной системы (АС) – классы АС, средства защиты информации необходимые для аттестации АС
24. Аттестация автоматизированной системы (АС) - основные работы при проведении аттестации
25. Специальные проверки - общие положения, термины и определения
26. Специальные исследования - общие положения, термины и определения
27. Российское программное обеспечение – операционная система МСВС
28. Аттестация программных ресурсов по требованиям защиты информации
29. Специальные исследования побочных электромагнитных излучений и наводок
30. Специальные исследования в области защиты речевой информации

31. Специальные исследования в области акустоэлектрических преобразований
32. Средства защиты от НСД (Secret Net 6.0) – назначение, возможности
33. Средства защиты от НСД (Страж 3.0) – назначение, возможности
34. Назначение и принцип работы прибора “вибро-шумомер “Октава 110А”
35. Назначение и принцип работы прибора “Детектор поля “ST-007”
36. Назначения и принцип работы “Электронный анализатор спектра “Agilent

Составитель _____ Шейдаков Н.Е.
(подпись)

«____»_____20 г.

Оформление тем рефератов (докладов, сообщений)

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

Кафедра *Информационных технологий и защиты информации*

Темы рефератов (докладов, сообщений)

по дисциплине Специальные методы исследования аппаратных средств информационных систем

1. Правовое обеспечение защиты государственной тайны
2. Правовая защита конфиденциальной информации
3. Нормативно-правовое регулирование профессиональной тайны
4. Нормативно-правовое регулирование служебной тайны
5. Правовое регулирование отношений по защите КТ на предпри-ятии
6. Правовые основы использования организационных и технических методов защиты информации
7. Правовые основы деятельности службы безопасности
8. Правовые основы использования технических средств сбора и защиты информации
9. Математическое и методическое обеспечение защиты объектов и источников информации
10. Криптография и стеганография – на службе защиты и кражи конфиденциальной информации.

11.Отечественные операционные системы на службе защиты IT-систем.
12.Российская операционная система Rosa Desktop
13.Операционная система «ОСь»
14.Какая операционная система нужна России?

Методические рекомендации по написанию, требования к оформлению

Содержание работы должно представлять обзор, анализ и обобщение материалов собранных из литературных источников сети Интернет, оформленных в соответствии с требованиями ГОСТ.

Критерии оценки:

- оценка «зачтено» выставляется студенту, *если работа соответствует полноте и содержательности проблемы исследования;, объем выполненных работы в полном объеме); соответствует требованиям по оформлению документа*
- оценка «не зачтено», *…если не выполнено одно из требований.*

Составитель _____ Н.Е. Шейдаков
(подпись)

«____»_____20 г.

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 зачета

Зачёт проводится по окончании теоретического обучения до начала экзаменационной сессии, как правило, на основе бально-рейтинговой системы по двум контрольным точкам в семестре.

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

«Специальные методы исследования аппаратных средств информационных систем»
(наименование дисциплины)

10.03.01 Информационная безопасность

10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель _____ Шейдаков Н.Е., доцент каф. ИТиЗИ, к.ф.-м.н., доцент.
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Специальные методы исследования аппаратных средств информационных систем» адресованы студентам очной формы обучения.

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

- практические занятия.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных при СР, развиваются навыки решения практических задач. При подготовке к практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- подготовить ответы на все вопросы по изучаемой теме;
- письменно решить домашние задания, рекомендованные преподавателем при изучении каждой темы.

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

По согласованию с преподавателем студент может подготовить реферат, доклад или сообщение по теме занятия.

Вопросы, не рассмотренные на лекциях должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины «Специальные методы исследования аппаратных средств информационных систем» осуществляется в ходе занятий методом устного опроса, проверки выполненных индивидуальных заданий, контрольных работ, 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.

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