

Аннотация к рабочей программе

дисциплины «Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций»

Цель дисциплины:

Дисциплина «Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций» относится к дисциплинам по выбору вариативной части учебного плана.

Дисциплина направлена на углубление знаний аспиранта по основным направлениям развития систем обеспечения информационной безопасности в инфокоммуникациях, знакомство с проблемами, определяющими дальнейший прогресс науки в этих областях, развитие навыков анализа и синтеза методов и средств защиты информации в системах и устройствах телекоммуникаций. Наряду с этим дисциплина способствует формированию у аспирантов научного мировоззрения, деловых качеств, свойственных научному работнику в области инфокоммуникаций и их информационной безопасности, а также развивает навыки правильной организации научно-исследовательской и преподавательской деятельности.

Основными задачами изучения дисциплины являются:

- актуализировать и углубить знания аспирантов по теоретическим и технологическим аспектам обеспечения информационной безопасности в инфокоммуникациях;
- расширение и углубление знаний по методологии выявления и решения научно-прикладных проблем в области информационной безопасности инфокоммуникаций;
- развить навыки системного подхода при изучении современных направлений развития систем связи, анализе научной информации необходимой для решения задач в научно-исследовательской деятельности;
- формирование умений и мотивирование к самостоятельной постановке задач и организации научно-исследовательской деятельности по совершенствованию методов и средств обеспечения информационной безопасности в инфокоммуникациях.

Компетенции, формируемые в результате освоения дисциплины

УК-1 - Способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях

ПК-2 - Способность разрабатывать новые и совершенствовать имеющиеся оптические методы доступа абонентов к ресурсам сетей, систем и устройств телекоммуникаций.

ПК-3 - Способность к исследованию, совершенствованию и разработке новых принципов организации данных и знаний в инфокоммуникациях, а также методов их проектирования

ПК-4 - Способность к исследованию и разработке новых методов защиты информации и обеспечению информационной безопасности в сетях, системах и устройствах телекоммуникаций

Разделы дисциплины:

1. Проблемы обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций
2. Основы теории защиты информации
3. Угрозы и оценка уязвимости информации в сетях, системах и устройствах телекоммуникаций
4. Требования к защите информации в сетях, системах и устройствах телекоммуникаций
5. Системы защиты информации в сетях, системах и устройствах телекоммуникаций
- 6 Развитие теории и практики защиты информации

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет



УТВЕРЖДАЮ:

Проректор по научной работе

Ю.Г. Добросердов

(подпись, инициалы, фамилия)

« 03 » 03 20 15 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций

(наименование дисциплины)

направления подготовки (специальность)

11.06.01

(шифр согласно ФГОС)

«Электроника, радиотехника и системы связи»

и наименование направления подготовки (специальности)

«Системы, сети и устройства телекоммуникаций»

наименование профиля, специализации или магистерской программы

форма обучения

очная


(очная, очно-заочная, заочная)

Курск – 2015

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» и на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» (направленность «Системы, сети и устройства телекоммуникаций»), одобренного Ученым советом университета протокол № 10 «29» июня 2015 г.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения аспирантов по направлению подготовки 11.06.01 «Электроника, радиотехника и системы связи» на заседании кафедры ЗИиСС «30» августа 2015 г., протокол № 1.

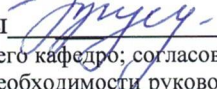
Зав. кафедрой

 к.т.н., с.н.с. профессор А.М. Потапенко

Разработчик программы д.т.н., доцент

 к.т.н., с.н.с. профессор А.М. Потапенко

Согласовано:

Начальник отдела докторантуры и аспирантуры  О.Ю. Прусова
(название кафедры, дата, номер протокола, подпись заведующего кафедрой; согласование производится с кафедрами чьи дисциплины основываются на данной дисциплине, а также при необходимости руководителями других структурных подразделений)

Директор научной библиотеки

 В.Г. Макаровская

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» направленность (профиль специализация) «Системы, сети и устройства телекоммуникаций», одобренного Ученым советом университета протокол № 11 «27» июня 2016 г., на заседании кафедры Космического приборостроения и систем связи 30.08.2016 г., протокол № 1

Зав. кафедрой

 С.Н. Михайлов


Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» направленность (профиль специализация) «Системы, сети и устройства телекоммуникаций», одобренного Ученым советом университета протокол № 10 «26» июня 2017 г., на заседании кафедры Космического приборостроения и систем связи 30.08.17 г., протокол № 1.

Зав. кафедрой

 А.Г. Андреев

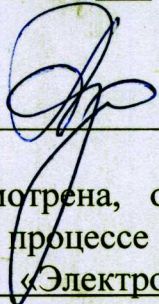
Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» направленность (профиль специализация) «Системы, сети и устройства телекоммуникаций», одобренного Ученым советом университета протокол № 12 «27» июня 2018 г., на заседании кафедры Космического приборостроения и систем связи 28.06.2018 г., протокол № 23.

Зав. кафедрой

 В.П. Андреев.

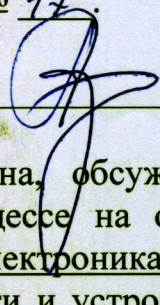
Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» (направленность «Системы, сети и устройства телекоммуникаций»), одобренного Ученым советом университета протокол № 9 от «24» 06 2019 г., на заседании кафедры Космического приборостроения и систем связи «26» 06 2019 г., протокол № 17.

Зав. кафедрой _____

 Андронов В.Г.


Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» (направленность «Системы, сети и устройства телекоммуникаций»), одобренного Ученым советом университета протокол № 11 от «29» 06 2020 г., на заседании кафедры Космического приборостроения и систем связи «07» 07 2020 г., протокол № 14.

Зав. кафедрой _____

 Андронов В.Г.

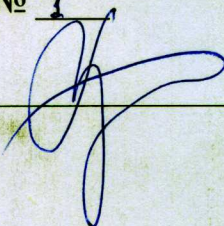
Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» (направленность «Системы, сети и устройства телекоммуникаций»), одобренного Ученым советом университета протокол № 8 от «31» мая 2021 г., на заседании кафедры Космического приборостроения и систем связи «02» июль 2021 г., протокол № 12.

Зав. кафедрой _____

 Андронов В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» (направленность «Системы, сети и устройства телекоммуникаций»), одобренного Ученым советом университета протокол № 11 от «27» 06 2022 г., на заседании кафедры Космического приборостроения и систем связи «31» 08 2022 г., протокол № 1.

Зав. кафедрой _____

 В.Г. Андронов

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» (направленность «Системы, сети и устройства телекоммуникаций), одобренного Ученым советом университета (протокол № 1 «31» 05 2021 г.), на заседании кафедры космического приборостроения и систем связи № 1 «31» 08 2023 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____



Андреев В. П.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» (направленность «Системы, сети и устройства телекоммуникаций), одобренного Ученым советом университета (протокол № « » 20 г.), на заседании кафедры космического приборостроения и систем связи № « » 202 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» (направленность «Системы, сети и устройства телекоммуникаций), одобренного Ученым советом университета (протокол № « » 20 г.), на заседании кафедры космического приборостроения и систем связи № « » 202 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана направления подготовки 11.06.01 «Электроника, радиотехника и системы связи» (направленность «Системы, сети и устройства телекоммуникаций), одобренного Ученым советом университета (протокол № « » 20 г.), на заседании кафедры космического приборостроения и систем связи № « » 202 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1 Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения ОП.

1.1. Цель преподавания дисциплины.

Целью преподавания данной дисциплины является изучение основных направлений развития систем обеспечения информационной безопасности в инфокоммуникациях, знакомство с проблемами, определяющими дальнейший прогресс науки в этих областях и основами их анализа и синтеза.

Наряду с этим преподавание дисциплины должно способствовать формированию у аспирантов научного мировоззрения, деловых качеств, свойственных научному работнику в области инфокоммуникаций и их информационной безопасности, а также развить навыки правильной организации научно-исследовательской и преподавательской деятельности.

1.2 Задачи изучения дисциплины

Основными задачами изучения дисциплины являются:

- актуализировать и углубить знания аспирантов по теоретическим и технологическим аспектам обеспечения информационной безопасности в инфокоммуникациях;
- расширение и углубление знаний по методологии выявления и решения научно-прикладных проблем в области информационной безопасности инфокоммуникаций;
- развить навыки системного подхода при изучении современных направлений развития систем связи, анализе научной информации необходимой для решения задач в научно-исследовательской деятельности;
- сформировать мотивационные установки и умения к самостоятельной постановке задач и организации научно-исследовательской деятельности по совершенствованию и разработке новых методов и средств обеспечения информационной безопасности в инфокоммуникациях.

1.3 Компетенции, формируемые в результате освоения дисциплины

ПК-3 - способностью к исследованию, совершенствованию и разработке новых принципов организации данных и знаний в инфокоммуникациях, а также методов их проектирования

ПК-4 - способностью к исследованию и разработке новых методов защиты информации и обеспечению информационной безопасности в сетях, системах и устройствах телекоммуникаций

Место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций» (Б1.В.ДВ.1.1) находится в вариативной части УП, в разделе «Дисциплины по выбору», изучается на 3 курсе, в 5 семестре.

3 Содержание и объем дисциплины»

3.1 Содержание дисциплины и лекционных занятий

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 час.

Таблица 3.1 –Объем дисциплины по видам учебных занятий

Объем дисциплины	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36.1
в том числе:	
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
экзамен	не предусмотрено
зачет	0,1
Аудиторная работа (всего):	36
в том числе:	
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
Самостоятельная работа обучающихся (всего)	72
Контроль/экзамен (подготовка к экзамену)	не предусмотрено

Таблица 3.2 – Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел, темы дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)	Компетенции
		№ лек., час	№ лаб., час	№ пр., час			
1	2	3	4	5	6	7	8
1	Проблемы обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций	1-2ч	0	1-2ч	У-1,2,3,7	С 5-6 неделя	ПК-3, ПК-4
2	Основы теории защиты информации	2-2ч	0	2-2ч	У-1,3,7,9	С 7 неделя	ПК-3, ПК-4
3	Угрозы и оценка уязвимости информации в сетях, системах и устройствах телекоммуникаций	3-2ч	0	3-2ч, 4-2ч, 5-2ч,	У-2,4,5,6,8,10,11	С 8 недели	ПК-4
4	Требования к защите информации в сетях, системах и устройствах телекоммуникаций	4-4ч	0	6-2ч	У-3,4,6,7,	С 9-10 недели	ПК-4
5	Системы защиты информации в	5-4ч	0	8-2	У-5,6 9	С	ПК-4

	сетях, системах и устройствах телекоммуникаций			9-2-ч		11 недели	
6	Развитие теории и практики защиты информации	6-4ч	0	10-2ч	У-1,4,5,6,8	С 12 недели	ПК-3, ПК-4
	всего	18	0	18			

Таблица 3.3 – Краткое содержание лекционного курса

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Проблемы обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций	Основные понятия и определения. Место информационной безопасности в современном обществе. Ретроспективный анализ и классификация подходов к защите информации. Постановка задачи защиты информации.
2	Основы теории защиты информации	Особенности и состав научно-методологического базиса решения задач защиты информации. Принципы и методологический базис теории защиты информации. Основное содержание теории защиты информации. Моделирование процессов защиты информации.
3	Угрозы и оценка уязвимости информации в сетях, системах и устройствах телекоммуникаций	Понятие угрозы безопасности информации. Подходы к формированию множества угроз. Классификация угроз безопасности информации. Методы оценки уязвимости информации. Модели оценки ущерба от реализации угроз безопасности информации
4	Требования к защите информации в сетях, системах и устройствах телекоммуникаций	Постановка задачи и анализ существующих методик определения требований к защите информации. Параметры защищаемой информации. Факторы, определяющие требуемый уровень защиты. Условия защиты информации.
5	Системы защиты информации в сетях, системах и устройствах телекоммуникаций	Определения, классификация систем защиты информации, стандартизация ее элементов. Проектирование систем защиты информации. Управление процессами функционирования систем защиты информации.
6	Развитие теории и практики защиты информации	Перспективы развития теории и практики защиты информации. Проблемы создания и организации работы центров защиты информации. Подготовка кадров в области обеспечения информационной безопасности.

3.2 Лабораторные работы и (или) практические занятия

Таблица 3.4 – Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности	2

	Место информационной безопасности в современном обществе. Подходы к защите информации в беспроводной радиосвязи.	
2	Защита информации в системах беспроводной связи путем имитозащиты передаваемых сообщений. Принципы формирования имитозащиты информации. Основное содержание теории защиты информации.	2
3	Методы сигнальной помехозащиты радиолиний. Понятие угрозы безопасности информации. Подходы к формированию множества угроз. Методы оценки уязвимости информации, формирования сигнальной помехозащиты.	6
4	Оценка помехозащиты спутниковой линии связи Постановка задачи и анализ существующих методик определения требований к защите информации спутниковой линии связи. Параметры защищаемой информации. Факторы, определяющие требуемый уровень защиты.	2
5	Оценка эффективности применения методов повышения скрытности РЭС Определения, классификация систем, методов защиты информации, стандартизация ее элементов.	4
6	Защита абонентского терминала в системе сотовой связи GSM Перспективы развития теории и практики защиты информации сотовых систем. Проблемы создания и организации работы центров защиты информации.	2
Итого		18

3.3 Самостоятельная работа аспирантов (СРС)

Таблица 3.6 – Самостоятельная работа студентов

№	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Проблемы обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций	5-6 неделя	10
2	Основы теории защиты информации	7 неделя	10
3	Угрозы и оценка уязвимости информации в сетях, системах и устройствах телекоммуникаций	8 недели	16
4	Требования к защите информации в сетях, системах и устройствах телекоммуникаций	9-10 недели	8
5	Системы защиты информации в сетях, системах и устройствах телекоммуникаций	11 недели	20
6	Развитие теории и практики защиты информации	12 недели	8
Итого			72

Общие методические указания к самостоятельной работе аспирантов изложены в Приложении Б.

4 Учебно-методическое обеспечение для самостоятельной работы

Аспиранты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:
 - методических рекомендаций, пособий по организации самостоятельной работы аспирантов;
 - заданий для самостоятельной работы;
 - тем рефератов и докладов;
 - вопросов к экзаменам и зачетам;
 - методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;
- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

5 Образовательные технологии

Таблица 5.1 – Образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Образовательные технологии	Объем, час.
1	2	3	4
1	Проблемы обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций	Лекция. Семинар: презентация и дискуссия	2 2
2	Основы теории защиты информации	Лекция. Семинар: презентация и дискуссия	2 2
3	Угрозы и оценка уязвимости информации в сетях, системах и устройствах телекомму-	Лекция с элементами проблемного изложения.	2

	никаций	Семинар: презентация и дискуссия	6
4	Требования к защите информации в сетях, системах и устройствах телекоммуникаций	Лекция с элементами проблемного изложения. Семинар: презентация и дискуссия	4 2
5	Системы защиты информации в сетях, системах и устройствах телекоммуникаций	Лекция с элементами проблемного изложения. Семинар: презентация и дискуссия	4 4
6	Развитие теории и практики защиты информации	Лекция с элементами проблемного изложения. Семинар: презентация и дискуссия	4 2
Итого:			36

6 Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 6.1 Этапы формирования компетенции

Код компетенции, содержание компетенции	Дисциплины (модули) при изучении которых формируется данная компетенция		
	Начальный	Основной	Завершающий
1	2	3	4
ОПК-3 - способностью к разработке новых методов исследования и их применению в самостоятельной профессиональной научно-исследовательской деятельности в области профессиональной деятельности	Б1.В.ОД.6 Системы, сети и устройства телекоммуникаций	Б1.В.ОД.4 Методология научных исследований при подготовке диссертации. Б1.В.ДВ.1.1 Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций В.ДВ.2.2 Модели и методы построения комплексных телекоммуникационных, измерительных и управляющих систем для мобильных приложений	Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
УК-1 - способностью к критическому анализу и оценке современных научных достижений, генерированию новых	Б1.В.ОД.6 Системы, сети и устройства телекоммуникаций	Б1.В.ДВ.2.2 Модели и методы построения комплексных телекоммуникационных, измерительных и управляющих систем для мобильных приложений	Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена. Б2.2 Научно-

идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях		ших систем для мобильных приложений	исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ПК-4 - способностью к исследованию и разработке новых методов защиты информации и обеспечению информационной безопасности в сетях, системах и устройствах телекоммуникаций	Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ОД.6 Системы, сети и устройства телекоммуникаций	Б1.В.ДВ.1.1 Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций Б1.В.ДВ.2.2 Модели и методы построения комплексных телекоммуникационных, измерительных и управляющих систем для мобильных приложений Б2.2 Научно-исследовательская практика	Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена. Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)

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

Таблица 6.2 Показатели и критерии определения уровня сформированности компетенций (частей компетенций)

№ п/п	Код компетенции (или её)	Уровни сформированности компетенции		
		Пороговый (удовлетворительный)	Продвинутый (хорошо)	Высокий (отлично)

	части)			
1	2	3	4	5
1	УК-1	<p>Знать: методики проведения анализа и оценок современных научных достижений</p> <p>Уметь: оценивать современные научные достижения.</p> <p>Владеть: способностью к критическому анализу.</p>	<p>Знать: методики проведения анализа и оценок современных научных достижений</p> <p>Уметь: оценивать современные научные достижения.</p> <p>Владеть: способностью к критическому анализу и произведению оценок современных научных достижений</p>	<p>Знать: методики проведения анализа и оценок современных научных достижений</p> <p>Уметь: оценивать современные научные достижения, генерирования новых идей при решении исследовательских и практических задач</p> <p>Владеть: способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях</p>
2	ОПК-3	<p>Знать: Основные этапы и сущность задач преобразования информации в инфокоммуникациях</p> <p>Уметь: производить классификацию угроз безопасности информации.</p> <p>Владеть: методикой определения требований по защите информации на различных этапах ее преобразования в инфокоммуникациях</p>	<p>Знать: основные проблемы обеспечения информационной безопасности на различных этапах преобразования информации в инфокоммуникациях.</p> <p>Уметь: определять цель, задачи объект и предмет преобразования и защиты информации на различных этапах ее преобразования в инфокоммуникациях</p> <p>Владеть: навыками формирования и обработки информационных ресурсов на различных этапах преобразования информации в инфокоммуникациях</p>	<p>Знать: принципы построения моделей процессов преобразования информации на прикладном, представительском, транспортном, канальном и физическом уровнях.</p> <p>Уметь: использовать теоретические и экспериментальные методы исследования, в том числе в междисциплинарных областях.</p> <p>Владеть: методами и средствами моделирования и проектирования систем преобразования информации на прикладном, представительском, транспортном, канальном и физическом уровнях</p>
3	ПК-4	<p>Методологию, сущность и содержание исследовательской деятельности в области</p>	<p>Знать: состояние развития науки и достижения в области информационной безопасно-</p>	<p>Знать: основные современные научные достижения в области информационной безопасно-</p>

	<p>информационной безопасности телекоммуникационных сетей, систем и устройств.</p> <p>Уметь: производить анализ научных достижений в области информационной безопасности инфокоммуникаций.</p> <p>Владеть: категориально-понятийным аппаратом в области развития в области информационной безопасности инфокоммуникаций.</p>	<p>сти инфокоммуникаций.</p> <p>Уметь: выявлять научные проблемы, определять цель, задачи и порядок проведения исследований в сфере информационной безопасности инфокоммуникаций.</p> <p>Владеть: методологией проектирования методов и средств защиты информации.</p>	<p>коммуникаций.</p> <p>Уметь: - определять методологию и порядок исследований по разработке методов и средств обработки и защиты информации на различных этапах её преобразования в инфокоммуникациях.</p> <p>Владеть: навыками математического и имитационного моделирования инфокоммуникационных сетей, систем и устройств.</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Таблица 6.3 Паспорт комплекта оценочных средств

№ п/п	Раздел (тема) дисциплины	Код компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Проблемы обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций	ПК-4	<p>Лекция</p> <p>Практическое занятие</p> <p>Лекция</p> <p>Практическое занятие</p>	Доклад с презентацией	1	<p>Оценивая ответ, члены комиссии учитывают следующие <i>основные критерии</i>:</p> <ul style="list-style-type: none"> – уровень теоретических знаний (подразумевается не только формальное воспроизведение информации, но и понимание предмета, которое подтверждается правильными ответами на дополнительные, уточняющие вопросы, заданные членами комиссии); – умение использовать теоретические знания при анализе конкретных проблем, ситуаций; – качество изложения материала, то есть обоснованность, четкость, логичность ответа, а также его полнота (то есть содержательность, не исключая сжатости); - способность устанавливать внутри- и межпредметные связи, оригинальность и красота мышления, зна-
2	Основы теории защиты информации	ОПК-3	<p>Лекция</p> <p>Практическое занятие</p>	Доклад с презентацией	2	

	мации		Лекция Практическое занятие	таци-ей		комство с дополнительной литературой и множество других факторов. <i>Критерии оценок:</i> Оценка <i>зачтено</i> – исчерпывающее владение программным материалом, понимание сущности рассматриваемых процессов и явлений, твёрдое знание основных положений дисциплины, умение применять концептуальный аппарат при анализе актуальных проблем. Логически последовательные, содержательные, конкретные ответы на все вопросы экзаменационного билета и на дополнительные вопросы членов комиссии, свободное владение источниками. Предложенные в качестве самостоятельной работы формы работы (примерный план исследовательской деятельности; пробная рабочая программа) приняты без замечаний.
3	Угрозы и оценка уязвимости информации в сетях, системах и устройствах телекоммуникаций	ПК-4	Лекция Практическое занятие Лекция Практическое занятие	До-клад с презентацией	3	Оценка <i>не зачтено</i> – отсутствие ответа хотя бы на один из основных вопросов, либо грубые ошибки в ответах, полное непонимание смысла проблем, не достаточно полное владение терминологией. Отсутствие выполненных самостоятельных дополнительных работ. Оценка по дисциплине «Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций» складывается из зачета самостоятельных работ и оценки ответа на зачете. <i>Показатели и критерии оценивания компетенций (результатов):</i> Процедура испытания предусматривает ответ аспиранта по вопросам зачетного билета, который заслушивает комиссия. После сообщения аспиранта и ответов на заданные вопросы, комиссия обсуждает качество ответа и голосованием принимает решение об оценке (зачтено/не зачтено), вносимой в протокол. Особое внимание обращается на степень осмысления процессов развития методологии науки и ее современных проблем.
4	Требования к защите информации в сетях, системах и устройствах телекоммуникаций	УК-1	Лекция Практическое занятие Сообщение студента	До-клад с презентацией	4	
5	Системы защиты информации в сетях, системах и устройствах телекоммуникаций	ПК-4	Лекция Практическое занятие Лекция Практическое занятие	Опрос	5	
6	Развитие теории и практики защиты ин-	ПК-4	Лекция Практическое занятие	Опрос	6	

	форма- ции		Лекция Практи- ческое занятие			Изучаемый материал должен быть по- нятым. Приоритет понимания обу- словливает способность изложения собственной точки зрения в контексте с другими позициями.
--	---------------	--	----------------------------------------	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

- раздел 6, таблицы 6.2, 6.3;
- приложения А, Б, В;
- оценочные средства представлены в учебно-методическом комплексе дисциплины.

6.3 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

1) Лекция с элементами проблемного изложения по вопросам:

«Проблемы обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций»;

«Основы теории защиты информации»;

«Угрозы и оценка уязвимости информации в сетях, системах и устройствах телекоммуникации»;

«Требования к защите информации в сетях, системах и устройствах телекоммуникаций»;

«Системы защиты информации в сетях, системах и устройствах телекоммуникаций»;

«Развитие теории и практики защиты информации».

При этом организация деятельности обучающегося должна строиться следующим образом:

- написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать важные мысли, выделять ключевые слова, термины. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

2) Доклад с презентацией Тема: «Проблемы обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций» по направлениям:

- фундаментальные предметные научные проблемы в сфере информационной безопасности инфокоммуникаций;

- фундаментальные технологические научные проблемы в сфере информационной безопасности инфокоммуникаций;

- прикладные предметные научные проблемы в сфере информационной безопасности инфокоммуникаций;

- проблемы технологические научные проблемы в сфере информационной безопасности инфокоммуникаций.

3) Доклад с презентацией Тема: «Основы теории защиты информации» по направлениям:

- классификация объектов и задач обеспечения информационной безопасности в инфокоммуникациях на:

прикладном,
представительском,
транспортном и сетевом,
канальном,
физическом уровнях.

- классификация методов и средств обеспечения информационной безопасности в инфокоммуникациях на:

прикладном,
представительском,
транспортном и сетевом,
канальном,
физическом уровнях.

4) Доклад с презентацией Тема: «Угрозы и оценка уязвимости информации в сетях, системах и устройствах телекоммуникаций».

- классификация угроз информационной безопасности в инфокоммуникациях;

- методы и средства реализации угроз информационной безопасности в инфокоммуникациях на:

прикладном,
представительском,
транспортном и сетевом,
канальном,
физическом уровнях.

- методы и средства математического моделирования инфокоммуникационных услуг, сетей, и систем;

- методы и средства имитационного моделирования инфокоммуникационных услуг, сетей, и систем.

5) Доклад с презентацией Тема: «Требования к защите информации

в сетях, системах и устройствах телекоммуникаций» на:

прикладном,
представительском,
транспортном и сетевом,
канальном,
физическом уровнях.

- состояние и основные направления повышения производительности линий связи на

6) Доклад с презентацией Тема: «Системы защиты информации в сетях, системах и устройствах телекоммуникаций» на:

прикладном,
представительском,
транспортном и сетевом,
канальном,
физическом уровнях.

7) Доклад с презентацией Тема: «Развитие теории и практики защиты информации» на:

прикладном,
представительском,

транспортном и сетевом,
канальном,
физическом уровнях.

8) Опрос.

Перечень вопросов приведен в приложении А

7 Рейтинговый контроль изучения дисциплины

Рейтинговый контроль не предусмотрен.

Описание оценочных средств и шкал оценивания ответов см. в Таблице 6.3.

8 Учебно-методическое и информационное обеспечение дисциплины

8.1 Основная и дополнительная учебная литература

1. Информационная безопасность и защита информации [Текст]: учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. – 384 с.
2. Крук, Борис Иванович. Телекоммуникационные системы и сети [Текст]: учебное пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В. П. Шувалова. - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком., - 2013. - Т. 1 : Современные технологии - 620 с.
3. Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации [Текст] : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - М. : Форум, 2013. - 256 с.
4. Абрамов, Г. В. Проектирование информационных систем [Электронный ресурс]: учебное пособие / Г. В. Абрамов, И. Медведкова, Л. Коробова. - Воронеж : Воронежский государственный университет инженерных технологий, 2012. - 172 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=141626>
5. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст]: учебное пособие / Е. А. Богданова [и др.]. - Москва: Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с.
6. Технические средства и методы защиты информации [Текст] : учебное пособие / под ред. А. П. Зайцева, А. А. Шелупанова. - М.: Горячая линия - Телеком, 2012. - 616 с.

8.2 Дополнительная литература:

7. Суглобов, Александр Евгеньевич. Экономическая безопасность предприятия [Текст]: учебное пособие / А. Е. Суглобов, С. А. Хмелев, Е. А. Орлова. - Москва : ЮНИТИ, 2014. - 271 с.
8. Советов, Б. Я. Моделирование систем [Текст]: учебник / Б. Я. Советов, С. А. Яковлев. - 5-е изд., стер. - М. : Высшая школа, 2007. - 343 с.
9. Применко, Эдуард Андреевич. Алгебраические основы криптографии [Текст]: учебное пособие / Э. А. Применко. - М. : Либроком, 2013. - 288 с. - (Основы защиты информации).
10. Фронтов, В. В. Регулирование телекоммуникаций в России и странах СНГ [Текст]: учебное пособие / В. В. Фронтов, В. О. Тихвинский. - М. : Горячая линия - Телеком, 2006. - 368 с.
11. Верзун Н. А. Множественный доступ в информационных системах [Текст]: учебное пособие / Н. А. Верзун ; Федеральное агентство связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. – СПб.: СПбГУТ, 2007.- 94 с.

8.3 Перечень методических указаний

1. Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности [Электронный ресурс]: методические указания по выполнению практической работы №1 по дисциплине «Методы и средства защиты информации и обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций» / Юго-Зап. гос. ун-т; сост.: А.М. Потапенко. - Электрон. текстовые дан. (КБ) Курск: ЮЗГУ, 2018. - 11с. - Б. ц.

2. Защита информации в системах беспроводной связи путем имитозащиты передаваемых сообщений [Электронный ресурс]: методические указания по выполнению практической работы № 2 по дисциплине «Методы и средства защиты информации и обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций» / Юго-Зап. гос. ун-т; сост.: А.М. Потапенко. - Электрон. текстовые дан. (КБ) Курск: ЮЗГУ 2018. 7 с. - Б. ц.

3. Методы сигнальной помехозащиты радиолиний [Электронный ресурс]: методические указания по выполнению практической работы № 3 «Методы и средства защиты информации и обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций» / Юго-Зап. гос. ун-т; сост.: А.М. Потапенко. - Электрон. текстовые дан. (КБ) Курск: ЮЗГУ, 2018. 8 с. - Б. ц.

4. Оценка помехозащиты спутниковой линии связи [Электронный ресурс]: методические указания по выполнению практической работы № 4 «Методы и средства защиты информации и обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций» / Юго-Зап. гос. ун-т; сост.: А.М. Потапенко. - Электрон. текстовые дан. (КБ) Курск: ЮЗГУ, 2018. 4 с. - Б. ц.

5. Оценка эффективности применения методов повышения скрытности РЭС [Электронный ресурс]: методические указания по выполнению практической работы № 5 «Методы и средства защиты информации и обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций» / Юго-Зап. гос. ун-т; сост.: А.М. Потапенко. - Электрон. текстовые дан. (КБ) Курск: ЮЗГУ, 2018. 12 с. - Б. ц.

6. Защита абонентского терминала в системе сотовой связи GSM [Электронный ресурс]: методические указания по выполнению практической работы № 6 «Методы и средства защиты информации и обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций» / Юго-Зап. гос. ун-т; сост.: А.М. Потапенко. - Электрон. текстовые дан. (КБ) Курск: ЮЗГУ, 2018. 8 с. - Б. ц.

8.4 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. <http://school-collection.edu.ru/> - федеральное хранилище Единая коллекция цифровых образовательных ресурсов.

2. <http://www.edu.ru/> - федеральный портал Российское образование.

3. <http://www.igumo.ru/> - интернет-портал Института гуманитарного образования и информационных технологий.

4. www.edu.ru – сайт Министерства образования РФ.

5. <http://elibrary.ru/defaultx.asp> - научная электронная библиотека «Elibrary».

6. <http://www.eduhmao.ru/info/1/4382/> - информационно-просветительский портал «Электронные журналы».

7. www.gumer.info – библиотека Гумер.

8. www.koob.ru – электронная библиотека Куб.

9. www.diss.rsl.ru – электронная библиотека диссертаций.

10. <http://fictionbook.ru> – электронная библиотека.

11. <http://svitk.ru> – электронная библиотека.

12. <http://www.iqlib.ru> – электронная библиотека образовательных и просветительных изда-

ний.

13. <http://www.integro.ru> - Центр Системных Исследований «Интегро».
14. <http://biblioteka.org.ua> – электронная библиотека
15. <http://www.lib.msu.su/index.html> - Научная библиотека Московского государственного университета им. М.В.Ломоносова.
16. <http://www.rsl.ru/> - Российская Государственная Библиотека.
17. <http://e.lanbook.com/> - Электронно-библиотечная система «Лань».
18. <http://www.iqlib.ru> - Электронно-библиотечная система IQLib.
19. <http://window.edu.ru/> - Электронная библиотека «Единое окно доступа к образовательным ресурсам».

8.5 Перечень информационных технологий

Чтение лекций с использованием слайд-презентаций.

Консультирование посредством электронной почты.

Использование слайд-презентаций при проведении научно-практических занятий.

9 Материально-техническое обеспечение дисциплины

В учебном процессе по дисциплине «Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций» задействованы аудитории, предназначенные для проведения лекций и практических занятий.

Предполагается использовать видеопроектор и ноутбук для показа презентаций и учебных фильмов.

10 Лист дополнений и изменений, внесенных в рабочую программу

Номер изменения	Номера страниц				Всего страниц	Дата	Основание* для изменения и подпись лица, проводившего изменения
	изменённых	заменённых	аннулированных	новых			

Примечание – Основанием для внесения изменения является решение кафедры (протокол №__ от ____).

Приложение А

к рабочей программе дисциплины

«Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций»

Вопросы к зачету по дисциплине

«Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций»

1. Определение и место информационной безопасности ТКС в общей совокупности информационных проблем современного общества.
2. Ретроспективный анализ развития подходов к защите информации.
3. Постановка задачи защиты информации.
4. Сущность, необходимость, пути и условия перехода к интенсивным способам защиты информации.
5. Особенности и состав научно-методологического базиса решения задач защиты информации в сетях, системах и устройствах телекоммуникаций.
6. Методологический базис теории защиты информации.
7. Принципы формирования теории защиты информации в сетях, системах и устройствах телекоммуникаций.
8. Основное содержание теории защиты информации в сетях, системах и устройствах телекоммуникаций .
9. Моделирование процессов защиты информации в сетях, системах и устройствах телекоммуникаций.
10. Понятие угрозы безопасности информации. Ретроспективный анализ подходов к формированию множества угроз.
11. Системная классификация угроз безопасности информации в сетях, системах и устройствах телекоммуникаций
12. Методы оценки уязвимости информации в сетях, системах и устройствах телекоммуникаций.
13. Модель нарушителя информационной безопасности.
14. Модели оценки ущерба от реализации угроз безопасности информации.
15. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты.
16. Субъектно-объектная модель доступа в сетях, системах и устройствах телекоммуникаций.
17. Политика безопасности и модели доступа. Многоуровневая политика безопасности MLS.
18. Определение, типизация и стандартизация систем защиты информации.
19. Проектирование систем защиты информации в ТКС. Управление процессами функционирования систем защиты ТКС.
20. Перспективы развития теории и практики защиты информации в инфокоммуникациях.

Приложение Б

к рабочей программе дисциплины

«Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций»

Методические указания для выполнения самостоятельной работы

Самостоятельная работа аспирантов направлена на:

- 1) совершенствование навыков восприятия и анализа проблемных вопросов развития инфокоммуникаций;
- 2) выработку навыков постановки научных проблем и задач;
- 3) овладение методами моделирования процессов формирования и преобразования телекоммуникационных сигналов;
- 4) развитие и совершенствование способностей к конструктивному диалогу, к дискуссии, к формированию логической аргументации и обоснованию собственной позиции по тому или иному вопросу.

Закрепление основных позиций в рамках дисциплины «Методы и средства защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций» должно строиться на понимании связи науки с философией, искусством, религией, социальной и практической деятельностью, а также с проблемами собственной специальности. Предполагается применение активных методов обучения, т.е. способы активизации учебно-познавательной деятельности аспирантов, которые побуждают их к активной мыслительной и практической деятельности в процессе овладения материалом. Активные методы обучения предполагают использование тематических таблиц и схем по учебной литературе, Интернет-материалов и лекций преподавателя, позволяющие оценить умение аспиранта работать с учебной литературой (выбирать, структурировать информацию, размещать её в хронологической последовательности).

Проверка выполнения заданий осуществляется как на семинарских занятиях с помощью устных выступлений и их коллективного обсуждения, так и с помощью письменных самостоятельных (контрольных) работ.

Для развития и совершенствования коммуникативных способностей аспирантов, навыков участия в конструктивном диалоге организуются специальные учебные занятия в виде, «диспутов» или «конференций», при подготовке к которым студенты заранее распределяются по группам, отстаивающим ту или иную точку зрения по обсуждаемой проблеме. Одним из видов самостоятельной работы является написание творческой работы по заданной либо согласованной с преподавателем теме. *Творческая работа (доклад с презентацией)* представляет собой оригинальное произведение объемом до 10 страниц печатного текста (10-15 слайдов), в данном случае предложено составление примерной *индивидуальной программы научного исследования*. Творческая работа не является рефератом, и не должна носить описательный характер. В ней желательно сосредоточить внимание на критическом анализе рассматриваемого материала и изложении своей точки зрения на проблему, что будет способствовать развитию творческих способностей. Так же в качестве самостоятельного задания аспирант подготавливает презентации по вопросам:

- постановки проблемы, формирования целей, темы, задач и развернутого плана диссертационных исследований;
- обобщенной и частных моделей исследуемых процессов.

Приложение В

к рабочей программе дисциплины
«Методы и средства защиты информации и обеспечение информационной безопасности в
сетях, системах и устройствах телекоммуникаций»

Методические указания аспиранту
по СР «Постановка задачи исследований ».

Выполнение самостоятельной семестровой работы направлено на приобретение практических навыков в работе с литературой по анализу и структурированию информации на примере выбранной темы диссертационной работы.

Самостоятельная семестровая работа должна включать в себя следующие элементы:

1. Обоснование актуальности направления исследований: выявление и формулирование существующего противоречия и имеющей место нерешенной проблемы (состояние вопроса на текущий момент (достигнутый уровень характеристик, степень внедрения, перспективные требования к основным функциям и характеристикам рассматриваемого объекта на современном этапе, степень несоответствия достигнутых характеристик новым требованиям)).
2. Анализ состояния вопроса по решению проблемы, вычленение нерешенных (недостаточно решенных) вопросов.
3. Определение объекта и предмета исследований;
4. Формулирование цели и основной научной задачи исследований.
5. Декомпозиция основной задачи на частные подзадачи и разработка структурно-логической схемы исследований – плана-проспекта диссертации.
6. Определение основных ожидаемых научных и практических результатов исследований.
7. Используемые источники информации (Не менее 50% источников должны быть не старше 5 лет).