МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

УТВЕРЖДАЮ
Директор Политехнического института
_____ Артамонов Д.В.
«_3_» _10_____ 2014 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

А1.В.ОД.5 «ПРОБЛЕМЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ»

Направление подготовки

10.06.01 Информационная безопасность

Направленность (профиль):

Методы и системы защиты информации, информационная безопасность

Квалификация (степень) – Исследователь. Преподаватель-исследователь.

Форма обучения: очная, заочная

Пенза, 2014

Рабочая программа «Проблемы и методы защиты информации в телекоммуникационных системах специального назначения» составлена в соответствии с требованиями ФГОС ВО по направлению 10.06.01 Информационная безопасность подготовки научно-педагогических кадров в аспирантуре.

Программу составил
Кашаев Е.Д., д.т.н., профессор _____

Программа обсуждена на заседании кафедры «Информационная безопасность систем и технологий»

Протокол № 1 от «16» 09 2014 года

Зав. кафедрой ИБСТ _____ С.Л. Зефиров
(подпись, Ф.И.О.)

Программа согласована с деканом факультета приборостроения, информационных технологий и электроники

Декан факультета ПИТЭ _____ В.Д. Кревчик
(подпись, Ф.И.О., дата)

Программа одобрена методической комиссией факультета ПИТЭ

Протокол № 1 от «1» 10 2014 года

Председатель методической комиссии
факультета ПИТЭ _____ А.В. Задера
(подпись, Ф.И.О.)

1. Цели и задачи изучения дисциплины

Цель изучения дисциплины – формирование у аспирантов углубленных профессиональных знаний о проблемах анализа, разработки, применения методов и средств защиты информации в телекоммуникационных системах специального назначения.

Задачи дисциплины:

- изучить основные методы и модели защиты информации в телекоммуникационных системах специального назначения;
- изучить основные угрозы информационной безопасности телекоммуникационных систем специального назначения;
- подготовить аспирантов к применению полученных знаний для анализа и разработки методов и средств защиты информации в телекоммуникационных системах специального назначения.

2. Место дисциплины в структуре ОПОП аспирантуры

Дисциплина относится к обязательным дисциплинам вариативной части учебного плана ООП по направлению подготовки 10.06.01 – Информационная безопасность, направленность (профиль) «Методы и системы защиты информации, информационная безопасность».

Изучение дисциплины базируется на следующих дисциплинах, формирующих определенные знания, умения и навыки:

1. Вычислительная техника и информационные технологии в профессиональной научной деятельности
2. Методы и средства защиты информации в условиях информационного противоборства
3. Информационная безопасность бизнеса и деятельности организации / Проблемы обеспечения информационной безопасности автоматизированных систем
4. Проблемы обеспечения безопасности информационной сферы организации

Основные положения дисциплины используются в следующих дисциплинах и практиках:

1. Методы и системы защиты информации, информационная безопасность
2. Практика по получению профессиональных умений и опыта профессиональной деятельности (научно-исследовательская практика)

Также основные положения дисциплины используются в процессе государственной итоговой аттестации, научно-исследовательской деятельности и при подготовке НКР (диссертации).

3. Компетенции аспиранта, формируемые в результате освоения программы дисциплины

Изучение дисциплины направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению подготовки:

Коды компетенции	Наименование компетенции	Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть)
1	2	3
ОПК-1	способность формулировать	*Знать:* основные методы и модели защиты

	научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	информации в телекоммуникационных системах специального назначения; основные угрозы информационной безопасности телекоммуникационных систем специального назначения
		Уметь: проводить классификацию, выделять и ранжировать угрозы информационной безопасности для конкретных телекоммуникационных систем и условий их эксплуатации
		Владеть: методологией проведения научных исследований и обобщения их результатов
ОПК-3	способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	*Знать:* действующие нормативные документы в области информационной безопасности
		Уметь: выбирать средства защиты информации и оценивать их возможности обеспечивать требуемый уровень защищенности
		Владеть: навыками анализа имеющихся методов и средств защиты информации
ПК-6	способность анализировать риски информационной безопасности, разрабатывать и применять современные методы обеспечения информационной безопасности в телекоммуникационных системах специального назначения	*Знать:* тенденции развития средств обеспечения информационной безопасности телекоммуникационных систем специального назначения
		Уметь: разрабатывать модели и алгоритмы защиты информации в телекоммуникационных системах специального назначения; проводить статистические исследования разработанных алгоритмов защиты информации в телекоммуникационных системах специального назначения
		Владеть: навыками планирования и оценки результатов статистических исследований
ПК-8	способность анализировать проблемы обеспечения безопасности информации ограниченного доступа и применять методы защиты информации при ее обработке в информационных системах	*Знать:* действующие нормативные документы в области защиты информации ограниченного доступа
		Уметь: применять методы защиты информации ограниченного доступа при ее обработке в информационных системах
		Владеть: навыками анализа проблем обеспечения безопасности информации ограниченного доступа

4. Структура и содержание дисциплины

4.1. Структура дисциплины

4.1.1. Структура дисциплины для очной формы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)*
				Аудиторная работа		Самостоятельная работа		
				Всего	Практические занятия	Всего	Подготовка к аудиторным занятиям	собеседование
1	*Раздел 1. Проблемы защиты информации в развернутых и перспективных телекоммуникационных системах специального назначения*	*6*	*1-5*	*6*	*6*	*18*	*18*	*1,3,5*
1.1	Тема 1.1 Методические, научно-технические и организационные проблемы защиты информации.	6	1	2	2	6	6	1
1.2	Тема 1.2 Информационный конфликт.	6	3	2	2	6	6	3
1.3	Тема 1.3 Обеспечение взаимоувязанности задач управления функциями передачи информации и функциями обеспечения информационной безопасности.	6	5	2	2	6	6	5
2	*Раздел 2. Проблемы разработки методов защиты информации в перспективных телекоммуникационных системах специального назначения*	*6*	*7-11*	*6*	*6*	*18*	*18*	*7,9,11*

2.1	Тема 2.1 Тенденции развития имеющихся методов и средств защиты информации.	6	7	2	2	6	6	7
2.2	Тема 2.2 Синтез интегрированных систем телекоммуникационных систем и обеспечение их информационной безопасности.	6	9	2	2	6	6	9
2.3	Тема 2.3 Разработка устройств защищенных телекоммуникационных систем специального назначения на базе отечественных сигнальных процессоров.	6	11	2	2	6	6	11
3	*Раздел 3. Методология исследований методов, моделей и алгоритмов защиты информации в телекоммуникационных системах специального назначения*	*6*	*13-17*	*6*	*6*	*18*	*18*	*13,15,17*
3.1	Тема 3.1 Проблемы натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами.	6	13	2	2	6	6	13
3.2.	Тема 3.2 Необходимость построения математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам нарушения информационной безопасности	6	15	2	2	6	6	15
3.3	Тема 3.3 Требования к методикам статистических исследований моделей, обеспечивающих полноту, точность и достоверность полученных результатов	6	17	2	2	6	6	17
	Общая трудоемкость, в часах			18	18	54	54	Промежуточная аттестация
								Форма: Зачет; Семестр: 6

4.1.2. Структура дисциплины для заочной формы
Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)*
				Аудиторная работа		Самостоятельная работа		
				Всего	Практические занятия	Всего	Подготовка к аудиторным занятиям	собеседование
1	*Раздел 1. Проблемы защиты информации в развернутых и перспективных телекоммуникационных системах специального назначения*	*6*	*1-5*	*3*	*3*	*21*	*21*	*1,3,5*
1.1	Тема 1.1 Методические, научно-технические и организационные проблемы защиты информации.	6	1	1	1	7	7	1
1.2	Тема 1.2 Информационный конфликт.	6	3	1	1	7	7	3
1.3	Тема 1.3 Обеспечение взаимоувязанности задач управления функциями передачи информации и функциями обеспечения информационной безопасности.	6	5	1	1	7	7	5
2	*Раздел 2. Проблемы разработки методов защиты информации в перспективных телекоммуникационных системах специального назначения*	*6*	*7-11*	*3*	*3*	*21*	*21*	*7,9,11*

2.1	Тема 2.1 Тенденции развития имеющихся методов и средств защиты информации.	6	7	1	1	7	7	7
2.2	Тема 2.2 Синтез интегрированных систем телекоммуникационных систем и обеспечение их информационной безопасности.	6	9	1	1	7	7	9
2.3	Тема 2.3 Разработка устройств защищенных телекоммуникационных систем специального назначения на базе отечественных сигнальных процессоров.	6	11	1	1	7	7	11
3	*Раздел 3. Методология исследований методов, моделей и алгоритмов защиты информации в телекоммуникационных системах специального назначения*	*6*	*13-17*	*3*	*3*	*21*	*21*	*13,15,17*
3.1	Тема 3.1 Проблемы натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами.	6	13	1	1	7	7	13
3.2.	Тема 3.2 Необходимость построения математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам нарушения информационной безопасности	6	15	1	1	7	7	15
3.3	Тема 3.3 Требования к методикам статистических исследований моделей, обеспечивающих полноту, точность и достоверность полученных результатов	6	17	1	1	7	7	17
	Общая трудоемкость, в часах			9	9	63	63	Промежуточная аттестация Форма: Зачет Семестр: 6

4.2. Содержание дисциплины

Раздел 1. Проблемы защиты информации в развернутых и перспективных телекоммуникационных системах специального назначения

Тема 1.1 Методические, научно-технические и организационные проблемы защиты информации.

Тема 1.2 Информационный конфликт.

Тема 1.3 Обеспечение взаимоувязанности задач управления функциями передачи информации и функциями обеспечения информационной безопасности.

Раздел 2. Проблемы разработки методов защиты информации в перспективных телекоммуникационных системах специального назначения

Тема 2.1 Тенденции развития имеющихся методов и средств защиты информации.

Тема 2.2 Синтез интегрированных систем телекоммуникационных систем и обеспечение их информационной безопасности.

Тема 2.3 Разработка устройств защищенных телекоммуникационных систем специального назначения на базе отечественных сигнальных процессоров.

Раздел 3. Методология исследований методов, моделей и алгоритмов защиты информации в телекоммуникационных системах специального назначения

Тема 3.1 Проблемы натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами.

Тема 3.2 Необходимость построения математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам нарушения информационной безопасности.

Тема 3.3 Требования к методикам статистических исследований моделей, обеспечивающих полноту, точность и достоверность полученных результатов.

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

1. Технология развития критического мышления реализуется в ходе проведения следующих видов учебной работы:

1.1. *Семинары-круглые столы*, в ходе которых происходит групповое обсуждение аспирантами учебной проблемы под руководством преподавателя. В ходе проведения круглого стола аспиранты приобретают навыки устного изложения заранее подготовленного материала, умение выслушивать коллег-сокурсников, делать заключения. В виде семинаров-круглых столов реализуются темы 1.1, 2.2, 2.3, 3.1, 3.3.

1.2. *Семинары-дискуссии*, в ходе которых обсуждается проблемная ситуация, поставленная преподавателем, а аспиранты защищают различные точки зрения на поставленную проблему. В ходе проведения дискуссии аспиранты приобретают умение излагать и аргументировано отстаивать точку зрения, обоснованно критиковать оппонентов, сопоставлять различные подходы к решению проблемной ситуации, делать выводы. В виде семинаров-дискуссий реализуются темы 1.2, 1.3, 2.1, 3.2.

2. Медиатехнология реализуется в ходе проведения следующих видов учебной работы:

2.1. *Семинары-круглые столы*, в ходе которых аспиранты делают краткие сообщения по рассматриваемой проблематике с использованием презентации. В результате использования этой технологии аспиранты учатся лаконично и ярко представлять информацию в аудитории. В виде семинаров-круглых столов с использованием медиатехнологий реализуются темы 1.1, 2.2, 2.3, 3.1, 3.3.

3. Кейс-технология реализуется в ходе проведения следующих видов учебной работы:

3.1. *Семинары-дискуссии*, в ходе которых в качестве одной из технологий используются такие приемы как мозговой штурм и дебаты. Мозговой штурм позволяет, используя групповую форму работы смоделировать процесс получения абсолютно новых для аспирантов знаний. Дебаты позволяют сопоставлять существующие противоположные подходы для решения одной и той же проблемы. В виде семинаров-дискуссий с использованием кейс-технологий реализуются темы 1.2, 1.3, 2.1, 3.2.

При организации самостоятельной работы используются следующие технологии:

1. Технология поиска и сбора новой информации (работа на компьютере с целью поиска информации в базах данных, работа с учебной, справочной и научной литературой с целью подготовки к семинарам: темы 1.1 – 3.3);

3. Технология анализа и представления новой информации (работа по подготовке устных сообщений на семинарах-круглых столах (темы 1.1, 2.2, 2.3, 3.1, 3.3), по подготовке для выступлений презентациями на семинарах-дискуссиях (темы 1.2, 1.3, 2.1, 3.2), по подготовке к зачету).

В целях реализации индивидуального подхода к обучению аспирантов, осуществляющих учебный процесс по собственной траектории в рамках индивидуального плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы с аспирантами, в том числе в электронной образовательной среде с использованием соответствующего программного оборудования, дистанционных форм обучения, возможностей интернет-ресурсов, индивидуальных консультаций и т.д.

6. Учебно-методическое обеспечение самостоятельной работы аспирантов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

6.1. План самостоятельной работы аспирантов

6.1.1 План самостоятельной работы аспирантов очной формы обучения

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Тема 1.1 Методические, научно-технические и организационные проблемы защиты информации	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [3]; дополнительная [1,2,5].	6
3	Тема 1.2 Информационный конфликт	Подготовка к аудиторным занятиям	Подготовка к семинару-дискуссии	основная [1,2,3]; дополнительная [1,2,3,6]	6
5	Тема 1.3 Обеспечение взаимоувязанности задач управления функциями передачи информации и функциями	Подготовка к аудиторным занятиям	Подготовка к семинару-дискуссии	основная [1,2,3]; дополнительная [1,2,3,6]	6

	обеспечения информационной безопасности				
7	Тема 2.1 Тенденции развития имеющихся методов и средств защиты информации	Подготовка к аудиторным занятиям	Подготовка к семинару-дискуссии	основная [1,2,3]; дополнительная [1,2,3,5,6]	6
9	Тема 2.2 Синтез интегрированных систем телекоммуникационных систем и обеспечение их информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [1,2,3]; дополнительная [1,2,6]	6
11	Тема 2.3 Разработка устройств защищенных телекоммуникационных систем специального назначения на базе отечественных сигнальных процессоров	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [1,2,3]; дополнительная [1,2,6]	6
13	Тема 3.1 Проблемы натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [1,2,3]; дополнительная [1,2,4]	6

	государствами				
15	Тема 3.2 Необходимость построения математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам нарушения информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к семинару-дискуссии	основная [1,2,3]; дополнительная [1,2,3,4,6]	6
17	Тема 3.3 Требования к методикам статистических исследований моделей, обеспечивающих полноту, точность и достоверность полученных результатов	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [1,2,3]; дополнительная [1,2,4]	6

6.1.2 План самостоятельной работы аспирантов заочной формы обучения

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Тема 1.1 Методические, научно-технические и организационные проблемы защиты информации	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [3]; дополнительная [1,2,5].	7
3	Тема 1.2 Информацион	Подготовка к аудиторным	Подготовка к семинару-	основная [1,2,3]; дополнительная	7

	ный конфликт	занятиям	дискуссии	[1,2,3,6]	
5	Тема 1.3 Обеспечение взаимоувязанности задач управления функциями передачи информации и функциями обеспечения информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к семинару-дискуссии	основная [1,2,3]; дополнительная [1,2,3,6]	7
7	Тема 2.1 Тенденции развития имеющихся методов и средств защиты информации	Подготовка к аудиторным занятиям	Подготовка к семинару-дискуссии	основная [1,2,3]; дополнительная [1,2,3,5,6]	7
9	Тема 2.2 Синтез интегрированных систем телекоммуникационных систем и обеспечение их информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [1,2,3]; дополнительная [1,2,6]	7
11	Тема 2.3 Разработка устройств защищенных телекоммуникационных систем специального назначения на базе отечественных сигнальных процессоров	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [1,2,3]; дополнительная [1,2,6]	7
13	Тема 3.1 Проблемы натурных испытаний перспективных	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [1,2,3]; дополнительная [1,2,4]	7

	защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами				
15	Тема 3.2 Необходимость построения математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам нарушения информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к семинару-дискуссии	основная [1,2,3]; дополнительная [1,2,3,4,6]	7
17	Тема 3.3 Требования к методикам статистических исследований моделей, обеспечивающих полноту, точность и достоверность полученных результатов	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу	основная [1,2,3]; дополнительная [1,2,4]	7

6.2. Методические указания по организации самостоятельной работы аспирантов

При изучении дисциплины самостоятельная работа аспирантов направлена на подготовку к практическим занятиям, проработку учебного материала по дисциплине.

6.3. Материалы для проведения текущего и промежуточного контроля знаний

6.3.1 Материалы для проведения текущего и промежуточного контроля знаний аспирантов очной формы обучения

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Собеседование	Тема 1.1 Методические, научно-технические и организационные проблемы защиты информации	ОПК-1
2	Собеседование	Тема 1.2 Информационный конфликт	ПК-6
3	Собеседование	Тема 1.3 Обеспечение взаимоувязанности задач управления функциями передачи информации и функциями обеспечения информационной безопасности	ОПК-3
4	Собеседование	Тема 2.1 Тенденции развития имеющихся методов и средств защиты информации	ОПК-1, ПК-8
5	Собеседование	Тема 2.2 Синтез интегрированных систем телекоммуникационных систем и обеспечение их информационной безопасности	ПК-6
6	Собеседование	Тема 2.3 Разработка устройств защищенных телекоммуникационных систем специального назначения на базе отечественных сигнальных процессоров	ПК-6
7	Собеседование	Тема 3.1 Проблемы натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами	ОПК-1
8	Собеседование	Тема 3.2 Необходимость построения математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам нарушения информационной безопасности	ОПК-1
9	Собеседование	Тема 3.3 Требования к методикам статистических исследований моделей, обеспечивающих полноту, точность и достоверность полученных результатов	ОПК-1

6.3.2 Материалы для проведения текущего и промежуточного контроля знаний аспирантов заочной формы обучения

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Собеседование	Тема 1.1 Методические, научно-технические и организационные проблемы защиты информации	ОПК-1
2	Собеседование	Тема 1.2 Информационный конфликт	ПК-6
3	Собеседование	Тема 1.3 Обеспечение взаимоувязанности задач управления функциями передачи информации и функциями обеспечения информационной безопасности	ОПК-3
4	Собеседование	Тема 2.1 Тенденции развития имеющихся методов и средств защиты информации	ОПК-1, ПК-8
5	Собеседование	Тема 2.2 Синтез интегрированных систем телекоммуникационных систем и обеспечение их информационной безопасности	ПК-6
6	Собеседование	Тема 2.3 Разработка устройств защищенных телекоммуникационных систем специального назначения на базе отечественных сигнальных процессоров	ПК-6
7	Собеседование	Тема 3.1 Проблемы натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами	ОПК-1
8	Собеседование	Тема 3.2 Необходимость построения математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам нарушения информационной безопасности	ОПК-1
9	Собеседование	Тема 3.3 Требования к методикам статистических исследований моделей, обеспечивающих полноту, точность и достоверность полученных результатов	ОПК-1

Вопросы для собеседования

Тема 1.1.

1. Нормативные документы.

2. Классы защищенности, грифы секретности.

3. Проблема организации взаимодействия общедоступных телекоммуникационных систем и систем специального назначения.

Тема 1.2.

1. Цели и задачи противоборствующих сторон в информационном конфликте.

2. Комплекс угроз защищенной телекоммуникационной системе на разных стадиях информационного конфликта.

3. Необходимость разработки комплекса взаимоувязанных средств обеспечения информационной безопасности телекоммуникационной системы.

4. Разработка алгоритмов адаптации защищенной телекоммуникационной системы к различным условиям и стадиям развития информационного конфликта.

Тема 1.3.

1. Декомпозиция защищенной телекоммуникационной системы на исполнительную, управляющую подсистемы и подсистему информационной безопасности.

2. Уязвимости исполнительной, управляющей подсистем и подсистемы информационной безопасности.

3. Системы радиоэлектронной борьбы.

Тема 2.1.

1. Анализ уязвимостей используемых методов защиты информации в телекоммуникационных системах в условиях конфликтного функционирования.

2. Необходимость разработки новых методов защиты, адекватных будущим угрозам информационной безопасности.

Тема 2.2.

1. Типовые средства, используемые для обеспечения функций передачи информации: защищенное оконечное оборудование данных, аппаратура передачи данных, маршрутизаторы, концентраторы, коммутаторы.

2. Типовые средства, используемые для обеспечения функций защиты информации.

3. Типовые средства, используемые для обеспечения функций управления.

Тема 2.3.

1. Уязвимости штатных средств на различных иерархических уровнях.

2. Способы повышения защищенности средств, реализующих функции передачи информации и управления.

3. Использование элементной базы повышенной надежности.

Тема 3.1.

1. Проведение натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами.

Тема 3.2.

1. Построение математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного информационного противодействия угрозам нарушения информационной безопасности.

2. Построение математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия активного информационного противодействия угрозам нарушения информационной безопасности.

Тема 3.3.

1. Методики статистических исследований моделей, обеспечивающих полноту, точность, своевременность и достоверность полученных результатов.

Вопросы и задания к зачету

1. Методические, научно-технические и организационные проблемы защиты информации.
2. Уязвимости используемых методов защиты информации в телекоммуникационных системах в условиях конфликтного функционирования.
3. Тенденции развития имеющихся методов и средств защиты информации.
4. Проблемы натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами.
5. Нормативные документы. Классы защищенности, грифы секретности.
6. Проблемы организации взаимодействия общедоступных телекоммуникационных систем и систем специального назначения.
7. Обеспечение полноты, точности и достоверности результатов статистических исследований моделей.
8. Цели и задачи противоборствующих сторон в информационном конфликте.
9. Угрозы телекоммуникационной системе специального назначения на разных стадиях информационного конфликта.
10. Алгоритмы адаптации телекоммуникационной системы специального назначения к различным условиям и стадиям развития информационного конфликта.
11. Обеспечение взаимоувязанности задач управления с функциями передачи информации и функциями обеспечения информационной безопасности.
12. Уязвимости исполнительной, управляющей подсистем и подсистемы информационной безопасности.
13. Системы радиоэлектронной борьбы иностранных государств.
14. Типовые средства, используемые для обеспечения функций защиты информации.
15. Способы повышения защищенности средств, реализующих функции передачи информации и управления.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

основная литература:

1. Куприянов, А.И. Теоретические основы радиоэлектронной разведки: учебное пособие / А.И. Куприянов, П.Б. Петренко. – М.: МГТУ им. Н.Э. Баумана (Московский государственный технический университет имени Н.Э. Баумана), 2009. – 388 с.

2. Куприянов, А.И. Радиоэлектронная борьба. Основы теории / А.И. Куприянов, Л.Н. Шустов. – М.: «Вузовская книга», 2011. – 800 с.

3. Конфликтно-устойчивые радиоэлектронные системы. Методы анализа и синтеза / Ю.А. Астапенко, С.Н. Вайпан, А.А. Вакуленко, Н.Н. Вакуленко, В.С. Верба, Р.А. Грибков, О.Б. Гузенко, В.Н. Дод, А.Г. Зайцев, А.А. Зебзеев, А.Н. Иванов, А.А. Ионкин, О.В. Король, Г.В. Кузьмин, В.Л. Лясковский, А.С. Марухленко, О.Н. Неплюев, И.А. Приступюк. – М.: Ридиотехника, 2015 г. – 312 с.

дополнительная литература:

1. Современная радиоэлектронная борьба. Вопросы методологии. / Под. Ред. В.Г. Радзиевского. – М.: «Радиотехника», 2006. – 424 с.

2. Энциклопедия «Оружие и технологии России. XXI век». Том 13 – «Системы управления, связи и радиоэлектронной борьбы» / Под общей редакцией МО РФ С. Иванова. – М.: ИД «Оружие и технологии», 2006.

3. Максимович Г.Ю. Информационные системы. Учебное пособие. Издательство: Российский государственный гуманитарный университет, 2007.

4. Советов Б. Я. Моделирование систем: учебник. Изд. 6-е. — М.: Высшая школа, 2009. — 343 с.

5. Доктрина информационной безопасности Российской Федерации 2016 г. https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

6. Радзиевский В.Г., Сирота А.А. Теоретические основы радиоэлектронной разведки. 2-е изд., испр. и доп. (1-е издание «Информационное обеспечение радиоэлектронных систем в условиях конфликта») – М.: «Радиотехника», 2004. – 432 с.

8. Материально-техническое обеспечение дисциплины (модуля)

Практические занятия проводятся в аудитории, оснащенной комплектом учебной мебели (стол преподавательский, парты, стулья, доска) и мультимедийной системой, состоящей из проектора, экрана настенного рулонного, ноутбука, с установленным свободно распространяемым программным обеспечением: операционная система Linux Debian 9; офисный пакет LibreOffice; программа просмотра pdf-документов Evince.

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата, подпись зав. кафедрой)	Внесенные изменения	Номера листов (страниц)		
			заменен-ных	новых	аннулиро-ванных
2015 – 2016	переутверждена пр-л №1 от 31.09.15	обновлён список осн. литературы	18	–	–
2016 – 2017	переутверждена пр-л №1 от 31.08.16	Без изменений			
2017 – 2018	переутверждена пр-л №1 от 31.08.17	Без изменений			