МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

А1.В.ОД.4 «МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

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

Программа дисциплины «Методы и системы защиты информации, информационная безопасность» составлена в соответствии с требованиями ФГОС ВО по направлению 10.06.01 «Информационная безопасность» подготовки научно-педагогических кадров в аспирантуре.

Программу составили:

1. Зефиров С.Л., к.т.н., зав.кафедрой _____

2. 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 методах, моделях, системах обеспечения и управления информационной безопасностью.

Задачи дисциплины:

- изучить методологические основы исследования проблем информационной безопасности объектов;
- изучить основные методы и системы защиты информации различных направлений обеспечения информационной безопасности;
- изучить основные методы и модели управления информационной безопасностью;
- подготовить аспирантов к применению полученных знаний для анализа моделей объектов и формирования моделей и методов управления и обеспечения информационной безопасности объектов

2. Место дисциплины в структуре ОПОП аспирантуры

Дисциплина относится к обязательным дисциплинам вариативной части блока А1.

Дисциплина предполагает наличие у аспирантов знаний по теории управления, теории принятия решений, теории информации, основам информационной безопасности, а также знаний и навыков, полученных аспирантами при изучении следующих дисциплинах учебного плана подготовки по направлению 10.06.01 "Информационная безопасность»: Информационная безопасность бизнеса и деятельности организации, Проблемы и методы защиты информации в телекоммуникационных системах специального назначения, Методы и средства защиты информации в условиях информационного противоборства

Знания и навыки, полученные аспирантами при изучении данной дисциплины, необходимы в научно-исследовательской практике, научно-исследовательской деятельности и подготовке НКР (диссертации) по направленности 05.13.19 – Методы и системы защиты информации, информационная безопасность

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 научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	*Знать:* - основные методы и модели обеспечения и управления информационной безопасностью; - методологические основы исследования проблем информационной безопасности объектов
		Уметь: - применять научно-методологический базис для моделирования и исследования объектов защиты; - применять методы и системы защиты

		информации для обеспечения информационной безопасности объектов
		Владеть: методологией рискориентированного подхода при анализе и исследовании методов и систем защиты информации
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 обеспечения информационной безопасности; - модели оценки информационной безопасности объектов
		Уметь: - выбирать модели и методы измерения и оценивания информационной безопасности объектов
		Владеть: навыками анализа и синтеза методов и моделей измерения и оценивания информационной безопасности в зависимости от целей и особенностей объекта защиты
ПК-4	Способность разрабатывать методы и модели информационной безопасности, проводить анализ защищенности и оценивать информационную безопасность объектов	*Знать:* - основные методы и модели обеспечения и управления информационной безопасностью; - модели оценки информационной безопасности объектов
		Уметь: - применять научно-методологический базис для моделирования и исследования объектов защиты; - разрабатывать и выбирать модели и методы измерения и оценивания информационной безопасности объектов
		Владеть: - методологией построения моделей и методов информационной безопасности объектов; - навыками анализа и синтеза методов и моделей измерения и оценивания информационной безопасности в зависимости от целей и особенностей объекта защиты
ПК-5	Способность анализировать риски информационной безопасности, разрабатывать и применять современные методы и модели информационной безопасности, оценки информационной безопасности автоматизированных систем	*Знать:* - модели и методы управления рисками информационной безопасности; - основные методы и модели обеспечения и управления информационной безопасностью; - модели оценки информационной безопасности объектов
		Уметь:

		- разрабатывать и применять методы и модели обеспечения и управления информационной безопасностью; - разрабатывать и применять методы и модели оценки информационной безопасности объектов
		Владеть: навыками анализа рисков информационной безопасности объектов, оценки информационной безопасности объектов
ПК-7	Способность создавать и исследовать модели систем защиты информации различного назначения, проводить анализ и обосновывать выбор решений по их применению	*Знать:* - значимость и свойства информации различного назначения в соответствии с целью объекта; - основные модели систем защиты информации различного назначения
		Уметь: - создавать и исследовать модели систем защиты информации различного назначения; - проводить анализ о возможности применения моделей систем защиты информации различного назначения
		Владеть: навыками обоснования решений по выбору и применению моделей систем защиты информации различного назначения

4. Структура и содержание дисциплины

4.1. Структура дисциплины

4.1.1. Структура дисциплины для очной формы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов

Экзамен по дисциплине проводится в формате кандидатского экзамена

№ 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 (*неделя*)	
				Аудиторная работа			Самостоятельная Работа				
				Всего	Лекция	Практические занятия	Всего	Подготовка к аудит. зан	Подготовка к экзамену	Собеседование	Контрол. работа
1	2	3	4	5	6	7	8	9	10	11	
	Раздел 1 Методологические основы исследования проблем информационной безопасности объектов										9
	Тема 1.1 Тема 1.2		1	2	2						
	Тема 1.3		2-3	4	2	2	8	8		2-3	
	Раздел 2 Методы и системы защиты информации										9
	Тема 2.1 Тема 2.2		4	3	1	2	5	5		4	

	Тема 2.3 Тема 2.4		5	3	1	2	5	5		5	
	Тема 2.5 Тема 2.6		6	1	1		5	5		6	
	Тема 2.7 Тема 2.8		7	1	1		5	5		7	
	Раздел 3 Методы и модели управления информационной безопасностью										16
	Тема 3.1 Тема 3.2		8	3	1	2	5	5		8	
	Тема 3.3 Тема 3.4		9-10	1	1		5	5		10	
	Тема 3.5 Тема 3.6		10-11	3	1	2	5	5		11	
	Тема 3.7 Тема 3.8		12	3	1	2	5	5		12	
	Раздел 4 Модели и методы обеспечения и управления информационной безопасностью										16
	Тема 4.1		13-14	4	2	2	8	8		13-14	
	Тема 4.2		15-16	4	2	2	8	8		15	
	Тема 4.3		17-18	4	2	2	8	8		17	
	Подготовка к экзамену						36				
	Общая трудоемкость, в часах			**36**	**18**	**18**	**108**	**72**	**36**	Пром. Аттест. Форма: Экз	Сем: 7

4.1.2. Структура дисциплины для заочной формы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов

Экзамен по дисциплине проводится в формате кандидатского экзамена

№ п/п	**Наименование разделов и тем дисциплины (модуля)**	**Семестр**	**Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (*в часах*)**					**Формы текущего контроля успеваемости**
			Аудиторная работа		**Самостоятельная Работа**			
			Всего	**Лекция**	**Всего**	**Подготовка к аудит. зан**	**Подготовка к экзамену**	**Собеседование**
1	**2**	**3**	**5**	**6**	**8**	**10**		**11**
	Раздел 1 Методологические основы исследования проблем информационной безопасности объектов		2	2	8	8		
	Тема 1.1 Тема 1.2	7	1	1	4	4		
	Тема 1.3	7	1	1	4	4		+
	Раздел 2 Методы и системы защиты информации		3	3	20	20		
	Тема 2.1 Тема 2.2	7	1	1	4	4		+
	Тема 2.3 Тема 2.4	7	1	1	4	4		+
	Тема 2.5 Тема 2.6	7	0,5	0,5	6	6		+
	Тема 2.7 Тема 2.8	7	0,5	0,5	6	6		+
	Раздел 3 Методы и модели управления информационной безопасностью		2	2	24	24		
	Тема 3.1 Тема 3.2	7	0,5	0,5	6	6		+
	Тема 3.3 Тема 3.4	7	0,5	0,5	6	6		+
	Тема 3.5 Тема 3.6	7	0,5	0,5	6	6		+
	Тема 3.7 Тема 3.8	7	0,5	0,5	6	6		+
	Раздел 4 Модели и методы обеспечения и управления информационной безопасностью		2	2	11	11		

	Тема 4.1	7	1	1	3	3		+	
	Тема 4.2	7	0,5	0,5	4	4		+	
	Тема 4.3	7	0,5	0,5	4	4		+	
	Подготовка к экзамену				36				
	Общая трудоемкость, в часах		**9**	**9**	**99**	**63**	**36**	Пром. Аттест.	
								Форма	Сем
								Экз	7

4.2. Содержание дисциплины

Раздел 1. Методологические основы исследования проблем информационной безопасности объектов

Тема 1.1 Информационные характеристики объектов защиты. Основные характеристики информационных систем, процессов. Характеристики, влияющие на информационную безопасность. Принципы обеспечения информационной безопасности объектов.

Тема 1.2 Стратегии защиты информации. Факторы, влияющие на формирование стратегий защиты. Классификационная структура множества необходимых стратегий защиты. Общая характеристика основных стратегий.

Тема 1.3 Научно-методологический базис для моделирования и исследования объектов защиты. Модели на основе нечётких множеств. Модели на основе марковских случайных процессов. Модели на основе теории игр. Модели, использующие положения нестрогой математики

Раздел 2. Методы и системы защиты информации

Тема 2.1 Защита информации от несанкционированного доступа (НСД). Каналы утечки информации. Системы анализа защищённости и обнаружения вторжений. Модели и источники каналов утечки информации.

Тема 2.2 Методы защиты программ от изучения и разрушающих программных воздействий. Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок; защита от разрушающих программных воздействий; изолированная программная среда.

Тема 2.3 Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом и физическом уровне от НСД. Методы защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации. Парольные системы опознавания, их сущность, содержание. Способы повышения надежности парольных систем. Средства опознавания аппаратуры, программ, массивов данных.

Тема 2.4 Методы идентификации и проверки подлинности пользователей систем. Идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных.

Тема 2.5 Биометрическая идентификация и аутентификация пользователей: основные понятия и механизмы. «Fuzzy extractors». Искусственные нейронные сети в преобразователях биометрия-код. Алгоритм быстрого обучения искусственной нейронной сети. Алгоритм ускоренного тестирования нейросетевого преобразователя биометрия-код (НПБК). Алгоритм полного тестирования НПБК. Базы биометрических образов: назначение, виды, требования к формированию. Нейросетевой биометрический контейнер (НБК): назначение, виды. Наиболее вероятные атаки на НБК, защита от них.

Тема 2.6 Программные средства разграничения доступа. Модели разграничения доступа. Разграничение доступа по уровням, матрицам полномочий и мандатам. Способы и средства повышения надежности разграничения. Программные средства защиты: регистрации, сигнализации, реагирования.

Тема 2.7 Организационно-правовые средства защиты, их сущность, возможности. Критерии классификации организационно-правовых средств, классификационная структура. Организационные мероприятия по защите информации, их сущность и назначение. Системная классификация организационных мероприятий. Мероприятия, проводимые на различных этапах жизненного цикла систем обработки данных.

Тема 2.8 Система законов, регламентирующих защиту информации в РФ. Перечень основных законов, основное их содержание и порядок действия. Руководящие методические материалы (РММ) по защите информации. Назначение и состав необходимых РММ. Перечень и содержание имеющихся РММ.

Раздел 3. Методы и модели управления информационной безопасностью

Тема 3.1 Необходимость, сущность управления информационной безопасностью. Создание, поддержка, оценка эффективности, совершенствование системы управления информационной безопасности.

Тема 3.2 Методы и модели управления рисками информационной безопасности. Итерационные процедуры управления рисками информационной безопасности.

Тема 3.3 Методы идентификации рисков информационной безопасности активов. Методы идентификации угроз информационной безопасности. Методы идентификации уязвимостей информационной безопасности.

Тема 3.4 Методы формирования сценариев инцидентов, модели сценариев инцидентов. Методы идентификации и анализа последствий инцидентов различного вида. Оценка ущерба в результате нарушения безопасности. Методы оценивания рисков информационной безопасности. Методы обработки рисков информационной безопасности. Оценка вариантов обработки рисков.

Тема 3.5 Методы управления изменениями систем.

Тема 3.6 Управление инцидентами информационной безопасности. Обнаружение и анализ инцидентов. Методы реагирования на инциденты информационной безопасности. Управление непрерывностью функционирования систем и объектов

Тема 3.7 Методы и модели мониторинга информационной безопасности. Структура систем мониторинга.

Тема 3.8 Модели и методы оценки информационной безопасности. Оценка соответствия защитных мер, процессов обеспечения информационной безопасности. Рискориентированная оценка информационной безопасности.

Раздел 4. Модели и методы обеспечения и управления информационной безопасностью

Тема 4.1 Информационная безопасность бизнеса и деятельности организации. Информационные аспекты бизнеса и деятельности организации. Факторы рисков информационной сферы организации. Модель информационной безопасности бизнеса и деятельности организации. Рискориентированный подход к обеспечению информационной безопасности. Модели рисков информационной безопасности. Методы снижения рисков информационной безопасности. Модели рискориентированной оценки информационной безопасности бизнеса и деятельности организации.

Тема 4.2 Информационная безопасность в условиях информационного противоборства. Концепции и цели информационного противоборства. Модели и методы информационного противоборства. Информационная война. Информационное оружие. Меры и средства, применяемые в качестве информационного оружия. Методы противодействия, реализуемые специальными системами защиты: безопасное межсетевое

взаимодействие, контроль и предотвращение утечек информации, защита информации в виртуальных инфраструктурах, методы, реализуемые специализированными операционными системами.

Тема 4.3 Защита информации в телекоммуникационных системах специального назначения. Обеспечение взаимоувязанности задач управления функциями передачи информации и функциями обеспечения информационной безопасности. Синтез интегрированных телекоммуникационных систем и обеспечение их информационной безопасности. Построение математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам нарушения информационной безопасности.

5. Образовательные технологии

В ходе освоения дисциплины «Методы и системы защиты информации, информационная безопасность» при проведении аудиторных занятий используются следующие образовательные технологии:

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

1.1. *Проблемные лекции*, которые предполагают диалоговый тип лекционного преподавания, предметом которого выступает вводимый лектором материал, отражающий основное содержание темы. В виде проблемных лекций реализуется темы 1.1, 1.2, 4.3

1.2. *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 участников семинара, делать заключения. В виде семинаров-круглых столов реализуются темы 1.3, 2.2, 2.4, 3.2, 3.6, 3.8, 4.1-4.3

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

2.1. Лекции, в ходе которых используются презентации, содержащие иллюстрации приводимых положений, элементы математических моделей. В виде лекций с использованием медиатехнологий реализуется все темы программы дисциплины.

2.2. *Семинары-круглые столы*, в ходе которых аспиранты делают краткие сообщения по рассматриваемой проблематике с использованием презентации. В результате использования этой технологии аспиранты учатся лаконично представлять информацию в аудитории. В виде семинаров-круглых столов с использованием медиатехнологий реализуются темы 1.3, 3.2, 3.6, 3.8, 4.1, 4.2.

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

№	Тема	Вид самостояте	Задание	Рекомендуемая литература	Количество

нед.		льной работы			часов
1-2	Тема 1.3 Научно-методологический базис для моделирования и исследования объектов защиты	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Модели на основе нечётких множеств. Модели на основе марковских случайных процессов»	Основная: 1, 2	8
3-4	Тема 2.2 Методы защиты программ от изучения и разрушающих программных воздействий	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение»	Основная: 3-6 Дополнительная: 5	5
5-6	Тема 2.4 Методы идентификации и проверки подлинности пользователей систем	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний»	Основная: 3-6 Дополнительная: 5	5
7-8	Тема 3.2 Методы и модели управления рисками информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Итерационные процедуры управления рисками информационной безопасности»	Основная: 7 Дополнительная: 2-4	5
9-10	Тема 3.6 Управление инцидентами информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Управление непрерывностью функционирования систем и объектов»	Дополнительная: 3-4	5
11-12	Тема 3.8 Модели и методы оценки информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Рискориентированная оценка информационной безопасности»	Основная: 7 Дополнительная: 3, 4	5
13-14	Тема 4.1 Информационная безопасность бизнеса и деятельности организации	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Факторы рисков информационной сферы организации. Модель информационной безопасности бизнеса и деятельности организации»	Основная: 1 Дополнительная: 2, 3	8
15-16	Тема 4.2 Информационная безопасность в условиях информационного противоборства	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Информационная война. Информационное оружие. Меры и средства, применяемые в качестве информационного оружия»	Основная: 7,8 Дополнительная: 1, 4	8
17-18	Тема 4.3 Защита информации в телекоммуникационных системах специального назначения	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Управление функциями передачи информации и функциями обеспечения информационной безопасности. Синтез интегрированных телекоммуникационных систем и обеспечение их информационной	Основная: 11-15 Дополнительная: 6	8

			безопасности»		

6.1.2 План самостоятельной работы аспирантов заочной формы обучения

№ сем	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
7	Тема 1.1, Тема 1.2	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Основные характеристики информационных систем, процессов, влияющие на информационную безопасность»	Основная: 1, 2	4
7	Тема 1.3	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Модели на основе нечётких множеств. Модели на основе марковских случайных процессов»	Основная: 1, 2	4
7	Тема 2.1, Тема 2.2	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение»	Основная: 3-6 Дополнительная: 5	4
7	Тема 2.3, Тема 2.4	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Идентификация и механизмы подтверждения подлинности пользователя»	Основная: 3-6 Дополнительная: 5	4
7	Тема 2.5, Тема 2.6	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Программные средства разграничения доступа. Модели разграничения доступа. Разграничение доступа по уровням, матрицам полномочий и мандатам»	Основная: 3-6 Дополнительная: 5	6
7	Тема 2.7, Тема 2.8	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Организационно-правовые средства защиты, их сущность, возможности. Критерии классификации организационно-правовых средств»	Основная: 3-6 Дополнительная: 5	6
7	Тема 3.1, Тема 3.2	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Итерационные процедуры управления рисками информационной безопасности»	Основная: 7 Дополнительная: 2-4	6
7	Тема 3.3, Тема 3.4	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Методы идентификации и анализа рисков»	Основная: 7 Дополнительная: 2-4	6
7	Тема 3.5, Тема 3.6	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Управление инцидентами информационной безопасности»	Дополнительная: 3,4	6
7	Тема 3.7, Тема 3.8	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Модели и методы оценки информационной безопасности»	Основная: 7 Дополнительная: 3, 4	6

7	Тема 4.1	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Факторы рисков информационной сферы организации. Модель информационной безопасности бизнеса и деятельности организации»	Основная: 1 Дополнительная: 2, 3	3
7	Тема 4.2	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Информационная война. Информационное оружие. Меры и средства, применяемые в качестве информационного оружия»	Основная: 7,8 Дополнительная: 1, 4	4
7	Тема 4.3	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Управление функциями передачи информации и функциями обеспечения информационной безопасности. Синтез интегрированных телекоммуникационных систем и обеспечение их информационной безопасности»	Основная: 11-15 Дополнительная: 6	4

6.2 Методические указания по организации самостоятельной работы аспирантов

6.2.1 Подготовка к аудиторным занятиям

Целью подготовки к аудиторным занятиям является предварительное ознакомление аспирантов с материалом источников для лучшего понимания и при проблемной лекции для участия в обсуждении лекционного материала и готовности к практическим занятиям в виде семинаров-круглых столов.

При подготовке к аудиторным занятиям необходимо пользоваться рекомендованными источниками, что не исключает необходимость самостоятельного подбора литературных источников по соответствующей тематике.

Подбор литературы в библиотечном фонде следует осуществлять с использованием алфавитного и системного каталогов. При подборе источников с использованием Интернет необходимо обращаться к профильным сайтам, тематическим форумам.

Полезно составлять конспекты, содержащие основные понятия, тезисы, выводы. При подготовке к практическим занятиям в виде семинаров-круглых столов может использоваться технология поиска и сбора новой информации в электронных базах данных, работа с учебной, справочной и научной литературой для подготовке устных сообщений и разработки презентаций для выступления и обсуждения материалов по теме семинаров.

Возникающие вопросы по рассматриваемому материалу необходимо отмечать в конспекте для последующей консультации с преподавателем.

Выводы, сформулированные по результатам рассмотрения материала, рекомендуется выделять для лучшего запоминания.

6.2.2 Подготовка к экзамену

При подготовке к экзамену аспирант осуществляет систематизацию имеющейся информации, сформированной на аудиторных занятиях и при подготовке к ним: работа с конспектом лекции, с конспектом практических занятий (семинаров).

6.3 Материалы для проведения текущего и промежуточного контроля знаний

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Собеседование	Разделы 1, 2, 3, 4	ОПК-1,3 ПК-4,5,7
2	Экзамен	Разделы 1, 2, 3, 4	ОПК-1,3 ПК-4,5,7

Демонстрационный вариант контрольной работы

Контрольная работа

Характеристики, влияющие на информационную безопасность объектов

Модели и источники каналов утечки информации

Вопросы для собеседования

Модели на основе теории игр

Способ идентификации событий информационной безопасности

Способы повышения надежности парольных систем

Виды и характеристики деструктивных информационных воздействий

Примерный перечень вопросов и заданий к экзамену

1. Особенности информатизации общества на современном этапе. Основные характеристики современных информационных систем. Необходимость обеспечения информационной безопасности систем и объектов.
2. Возникновение проблемы защиты информации. Развитие и становление способов защиты. Этапы развития и их характеристики.
3. Определение, особенности и общее содержание теории защиты информации.
4. Научно-методологический базис теории защиты. Система моделей защиты информации.
5. Определение и основные понятия стратегии защиты информации. Факторы, влияющие на формирование стратегий защиты. Классификационная структура множества необходимых стратегий защиты. Общая характеристика основных стратегий.
6. Определение и назначение инструментально-методологического базиса защиты информации. Требования к инструментально-методологическому базису.
7. Пути и способы реализации основных положений теории защиты информации.
8. Перспективы и проблемы развития теории и практики защиты.
9. Определение и природа угроз информации в современных системах ее обработки.
10. Классификация и общая характеристика основных угроз.
11. Понятие уязвимости информации. Подходы к определению значений показателей уязвимости.
12. Эмпирические методы определения значений показателей уязвимости. Примеры эмпирических моделей. Способы определения параметров моделей. Особенности использования моделей.
13. Теоретико-вероятностные методы определения значений показателей уязвимости, подходы к построению моделей. Примеры моделей. Особенности и проблемы практического использования.
14. Теоретико-эмпирические методы определения значений показателей. Подходы к построению теоретико-эмпирических моделей. Понятие базового показателя уязвимости, аналитическая и статистическая модели его определения.
15. Методы и модели прогнозирования значений показателей уязвимости.
16. Определение, значение, структура и способы формирования инструментальных средств оценки уязвимости информации.
17. Защита автоматизированных систем от удаленных атак через сеть Internet.

18. Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов;

19. Применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

20. Защита информации от несанкционированного доступа (НСД). Защита компонентов автоматизированных систем от НСД.

21. Антивирусная защита.

22. Системы анализа защищённости и обнаружения вторжений.

23. Каналы утечки информации. Модель и источники каналов утечки информации.

24. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).

25. Классификация способов защиты от изучения и разрушающих программных воздействий; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение.

26. Защита от разрушающих программных воздействий; понятие изолированной программной среды.

27. Понятие разрушающего программного воздействия; компьютерные вирусы как особый класс разрушающих программных воздействий.

28. Модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок.

29. Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.

30. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации.

31. Парольные системы опознавания, их сущность, содержание, достоинства и недостатки. Способы повышения надежности парольных систем.

32. Другие системы опознавания. Средства опознавания аппаратуры, программ, массивов данных.

33. Методы идентификации и проверки подлинности пользователей автоматизированных систем.

34. Методы идентификации и проверки подлинности пользователя системы. Идентификация и механизм подтверждения подлинности пользователя, взаимная проверка подлинности пользователей

35. Протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных.

36. Биометрическая идентификация и аутентификация пользователей: основные понятия и механизмы. «Fuzzy extractors».

37. Искусственные нейронные сети в преобразователях биометрия-код. Алгоритм быстрого обучения искусственной нейронной сети.

38. Алгоритм ускоренного тестирования нейросетевого преобразователя биометрия-код (НПБК). Алгоритм полного тестирования НПБК.

39. Базы биометрических образов: назначение, виды, требования к формированию. Нейросетевой биометрический контейнер (НБК): назначение, виды. Наиболее вероятные атаки на НБК, защита от них.

40. Программные средства разграничения доступа, их сущность, достоинства и недостатки.

41. Модели разграничения доступа. Разграничение доступа по уровням и кольцам секретности, матрицам полномочий и мандатам. Способы и средства повышения надежности разграничения.

42. Примеры систем разграничения доступа. Другие программные средства защиты: регистрации, сигнализации, реагирования и т.п.

43. Программы защиты ЭВМ от электронных вирусов.

44. Способы организации и использования программных средств защиты.

45. Организационно-правовые средства защиты, их сущность, возможности, достоинства и недостатки.

46. Критерии классификации организационно-правовых средств, классификационная структура и общая характеристика.

47. Система законов, регламентирующих защиту информации в РФ. Перечень основных законов, основное их содержание и порядок действия.

48. Руководящие методические материалы (РММ) по защите информации. Назначение и состав необходимых РММ. Перечень и содержание имеющихся РММ.

49. Организационные мероприятия по защите информации, их сущность и назначение.

50. Системная классификация организационных мероприятий. Мероприятия, проводимые на различных этапах жизненного цикла систем обработки данных.

51. Стеганография. Основы стеганографии. Основные понятия. Компьютерная стеганография.

52. Необходимость, сущность и основные понятия управления информационной безопасностью.

53. Служба информационной безопасности на объекте. Назначение и организационно-правовой статус службы. Функции и задачи службы, способы и методы их решения.

54. Создание, поддержка, оценка эффективности, совершенствование системы управления информационной безопасности.

55. Модели и методы оценки информационной безопасности

56. Методы и модели управления рисками информационной безопасности. Формирование критериев влияния, оценивания, принятия рисков. Итерационные процедуры управления рисками информационной безопасности.

57. Методы и модели оценки рисков информационной безопасности. Методы идентификации рисков информационной безопасности активов. Методы формирования сценариев инцидентов, модели сценариев инцидентов. Методы идентификации и анализа последствий инцидентов различного вида.

58. Оценка ущерба в результате нарушения безопасности. Методы оценивания рисков информационной безопасности. Методы обработки рисков информационной безопасности. Оценка вариантов обработки рисков.

59. Оценка эффективности выбранных защитных мер. Методы управления изменениями систем.

60. Управление инцидентами информационной безопасности. Обнаружение и анализ инцидентов. Методы реагирования на инциденты информационной безопасности.

61. Управление непрерывностью функционирования систем и объектов

62. Методы и модели мониторинга информационной безопасности. Структура систем мониторинга.

63. Методы аудита информационной безопасности. Оценка соответствия защитных мер, процессов обеспечения информационной безопасности. Методы выявления и анализа свидетельств оценки.

64. Организация обучения и осведомления персонала информационной безопасности.

65. Математические модели исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам информационной безопасности

66. Защита информации в телекоммуникационных системах специального назначения, обеспечение взаимосвязанности задач управления функциями передачи информации с функциями обеспечения информационной безопасности

6. Рекомендуемая литература

6.1. Основная литература

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.
2. Расторгуев С.П. Математические модели в информационном противоборстве. Экзистенциальная математика. – Электрон. дан. — М.: АНО ЦСОиП, 2014. – 260 с. – Режим доступа: csef.ru/media/articles/5310/5310.pdf. – Загл. с экрана.
3. Леандро, К. Windows Server 2012 Hyper-V. Книга рецептов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2013. — 302 с. — Режим доступа: https://e.lanbook.com/book/58692. — Загл. с экрана.

4 Коробко, И.В. PowerShell как средство автоматического администрирования [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2012. — 224 с. — Режим доступа: https://e.lanbook.com/book/4818. — Загл. с экрана.

5 Михеев, М.О. Администрирование VMware vSphere [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2012. — 504 с. — Режим доступа: https://e.lanbook.com/book/9124. — Загл. с экрана.

6. Чипига А.Ф. Информационная безопасность автоматизированных систем. – М.: Гелиос-АРВ, 2010.
7. Хорев П.Б. Программно-аппаратная защита информации. – М.: Форум, 2009.
8. Обеспечение информационной безопасности бизнеса/В.В.Андрианов, С.Л.Зефиров, В.Б.Голованов, Н.А.Голдуев. – М.: Альпина Паблишерс, 2011. – 373с.
9. Общая теория рисков: учеб. пособие для студ. высш. учеб. заведений/ Я.Д.Вишняков, Н.Н.Радаев. – М.: Издательский центр «Академия», 2008. – 368с.
10. Современная радиоэлектронная борьба. Вопросы методологии. / Под. Ред. В.Г. Радзиевского. – М.: «Радиотехника», 2006. – 424 с.
11. 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.
12. 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.
13. Куприянов, А.И. Радиоэлектронная борьба. Основы теории / А.И. Куприянов, Л.Н. Шустов. – М.: «Вузовская книга», 2011. – 800 с.
14. 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.

6.2 Дополнительная литература

1. Информационная безопасность систем организационного управления. Теоретические основы [Текст]: в 2т/ Н.А.Кузнецов, В.В.Кульба, Е.А.Микрин и др. Институт проблем передачи информации РАН. – М.: Наука, 2006. Библиотека кафедры ИБСТ

1 экз.

2. ГОСТ Р ИСО/МЭК 27001 Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Требования [Электронный ресурс]

http://www.internet-law.ru/gosts/gost/5736/

3. ГОСТ Р ИСО/МЭК 27002 Информационная технология – Методы и средства обеспечения безопасности – Свод норм и правил менеджмента информационной безопасности [Электронный ресурс]

http://www.internet-law.ru/gosts/gost/54705

4. ГОСТ Р ИСО/МЭК 27004 Информационная технология – Методы и средства обеспечения безопасности – Менеджмент информационной безопасности – Измерения [Электронный ресурс]

http://www.internet-law.ru/gosts/gost/514

5. 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. Библиотека кафедры ИБСТ

1 экз.

6. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2012. — 592 с. — Режим доступа: https://e.lanbook.com/book/3032. — Загл. с экрана.

7. Галатенко В.А. Основы информационной безопасности : [Текст] учебное пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. - 4-е изд. - М. : Интернет - Ун-т Информационных Технологий : БИНОМ. Лаборатория знаний, 2012. - 205 с. – 2 экз.

http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=14831

6.3 Интернет-ресурсы

1. www.elibrary.ru,
2. www.elsv.ru
3. www.cnews.ru – ресурс, содержащий материалы об информационных технологиях и обеспечении ИБ
4. www.servernews.ru – информационные материалы о средствах ИТ и средствах обеспечения ИБ
5. www.fstec.ru – сайт ФСТЭК РФ
6. www.infosec.ru – группа компаний Информзащита
7. www.anti-malware.ru – аналитический центр Anti-Malware.ru

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	пр-л №1 от 3.09.15	Без изменений			
2016-2017	пр-л №1 от 8.09.16	обновлён раздел 6	14, 15		
2017-2018	пр-л №1 от 31.08.17	Без изменений			