МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

УТВЕРЖДАЮ
Директор Политехнического института
_____ Артамонов Д.В.
«31» 10 2014 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

А1.В.ДВ2.1 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА И ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИЙ»

Направление подготовки

10.06.01 Информационная безопасность

Направленность (профиль):

Методы и системы защиты информации, информационная безопасность

Квалификация (степень) – Исследователь. Преподаватель-исследователь.

Форма обучения очная и заочная

Пенза, 2014

Рабочая программа дисциплины «Информационная безопасность бизнеса и деятельности организации» составлена в соответствии с требованиями ФГОС ВО по направлению 10.06.01 «Информационная безопасность» подготовки научно-педагогических кадров в аспирантуре (уровень подготовки кадров высшей квалификации).

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 моделях и методах управления информационной безопасностью бизнеса (деятельности).

Задачи дисциплины:

- изучить основные компоненты моделей и методы информационной безопасности бизнеса (деятельности);
- изучить основные источники рисков информационной безопасности в информационной сфере объектов и способы управления ими;
- подготовить аспирантов к применению полученных знаний для анализа информационных моделей объектов и формирования модели и методов управления информационной безопасностью объектов

2. Место дисциплины в структуре ОПОП аспирантуры

Дисциплина относится к дисциплинам по выбору вариативной части блока А1.

Дисциплина предполагает наличие у аспирантов знаний по теории управления, теории принятия решений, общей теории управления и обеспечения информационной безопасности.

Знания и навыки, полученные аспирантами при изучении данной дисциплины, необходимы при изучении дисциплин:

– Методы и средства защиты информации в условиях информационного противоборства,

– Методы и системы защиты информации, информационная безопасность,

а также при подготовке к государственному экзамену, в научно-исследовательской деятельности и 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 научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	*Знать:* - компоненты моделей и методы управления информационной безопасностью бизнеса (деятельности); - основные источники рисков в информационной сфере организации, модели управления рисками
		Уметь: - определить компоненты модели информационной безопасности бизнеса (деятельности) в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы; - определить факторы рисков

		информационной безопасности бизнеса (деятельности) и сформировать факторную модель управления информационной безопасностью организации.
		Владеть: методологией рискориентированного подхода при анализе и исследовании системы управления информационной безопасности
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 управления информационной безопасностью; - модель процессов управления информационной безопасностью, их значимость и влияние на достижение целей информационной безопасности бизнеса (деятельности)
		Уметь: - определить процессы и подпроцессы управления информационной безопасностью бизнеса (деятельности) в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы; - выбирать модели и методы измерения и оценивания информационной безопасности в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы
		Владеть: навыками анализа и синтеза методов и моделей измерения и оценивания информационной безопасности в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы
ПК-4	Способность разрабатывать методы и модели информационной безопасности, проводить анализ защищенности и оценивать информационную безопасность объектов	*Знать:* - действующие нормативные документы в области оценки информационной безопасностью
		Уметь: - разрабатывать и выбирать модели и методы измерения и оценивания информационной безопасности в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы
		Владеть: навыками анализа и синтеза методов и моделей измерения и оценивания информационной безопасности в зависимости от целей

		бизнеса в информационной сфере и особенностей информационной сферы
ПК-5	Способность анализировать риски информационной безопасности, разрабатывать и применять современные методы и модели обеспечения информационной безопасности, оценки информационной безопасности автоматизированных систем	*Знать:* методы анализа и оценки рисков информационной безопасности автоматизированных систем
		Уметь: - разрабатывать модели информационной безопасности автоматизированных систем в зависимости от целей систем и их особенностей; - определить метод оценки информационной безопасности автоматизированных систем в зависимости от целей оценки и особенностей систем.
		Владеть: методиками оценки информационной безопасности автоматизированных систем
ПК-7	Способность создавать и исследовать модели систем защиты информации различного назначения, проводить анализ и обосновывать выбор решений по их применению	*Знать* модели управления информационной безопасностью систем различного назначения
		Уметь: - разрабатывать модели информационной безопасности автоматизированных систем в зависимости от назначения
		Владеть: методиками анализа и оценки информационной безопасности автоматизированных систем

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

№ 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 аудитор. зан	Подготовка к экзамену	Собеседование
	Раздел 1. Бизнес и информация			8	4	4	8	8		4
	Тема 1.1 Информационная основа бизнеса (деятельности) организации	1	1-2	4	2	2	4	4		

	Тема 1.2 Информационные характеристики бизнеса	1	3-4	4	2	2	4	4			
	Раздел 2. Модель информационной безопасности бизнеса			8	4	4	8	8		8	
	Тема 2.1 Общая структура информационной сферы. Связь с материальным миром	1	5-6	4	2	2	4	4			
	Тема 2.2 Эволюция моделей информационной безопасности бизнеса. Риски, рисковые события, ущербы и уязвимости	1	7-8	4	2	2	4	4			
	Раздел 3. Основные источники рисков в информационной сфере организации			12	6	6	12	12		12,14	
	Тема 3.1 Сложность информационной сферы	1	9-10	4	2	2	4	4			
	Тема 3.2 Неточность отображения материального мира в информационные модели	1	11-12	4	2	2	4	4			
	Тема 3.3 Конфликт интересов. Управление информационной безопасностью, связанной с персоналом	1	13-14	4	2	2	4	4			
	Раздел 4. Основные модели и методы управления информационной безопасностью			8	4	4	8	8		17	
	Тема 4.1 Процессы управления информационной безопасностью бизнеса (деятельности) в зависимости от целей бизнеса в информационной сфере	1	15-16	4	2	2	4	4			
	Тема 4.2 Модели и методы измерения и оценивания информационной безопасности	1	17-18	4	2	2	4	4			
	Подготовка к экзамену						36				
	Общая трудоемкость, в часах			**36**	**18**	**18**	**72**	**36**	**36**	Пром. аттест.	
										Форма	Сем
										Зач	
										Экз	1

4.1.2. Структура дисциплины для заочной формы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов

№ 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	**Лекции**	**Всего**	**Подготовка к аудиторным зан**	**Подготовка к экзамену**	**Собеседование**
	Раздел 1. Бизнес и информация	1	2	2	12	12		
	Тема 1.1 Информационная основа бизнеса (деятельности) организации		1	1	6	6		
	Тема 1.2 Информационные характеристики бизнеса		1	1	6	6		+

	Раздел 2. Модель информационной безопасности бизнеса	1	2	2	14	14			
	Тема 2.1 Общая структура информационной сферы. Связь с материальным миром		1	1	6	6		+	
	Тема 2.2 Эволюция моделей информационной безопасности бизнеса. Риски, рисковые события, ущербы и уязвимости		1	1	8	8		+	
	Раздел 3. Основные источники рисков в информационной сфере организации	1	3	3	22	22			
	Тема 3.1 Сложность информационной сферы		1	1	7	7		+	
	Тема 3.2 Неточность отображения материального мира в информационные модели		1	1	7	7		+	
	Тема 3.3 Конфликт интересов. Управление информационной безопасностью, связанной с персоналом		1	1	8	8		+	
	Раздел 4. Основные модели и методы управления информационной безопасностью	1	2	2	15	15			
	Тема 4.1 Процессы управления информационной безопасностью бизнеса (деятельности) в зависимости от целей бизнеса в информационной сфере		1	1	7	7		+	
	Тема 4.2 Модели и методы измерения и оценивания информационной безопасности		1	1	8	8		+	
	Подготовка к экзамену				36		36		
	Общая трудоемкость, в часах		**9**	**9**	**99**	**63**	**36**	Пром. аттест.	
								Форма	Сем
								Зач	
								Экз	1

4.2. Содержание дисциплины

Лекционные занятия

Раздел 1. Бизнес и информация

Тема 1.1 Информационная основа бизнеса (деятельности) организации

Тема 1.2 Информационные характеристики бизнеса

Раздел 2. Модель информационной безопасности бизнеса

Тема 2.1 Общая структура информационной сферы. Связь с материальным миром

Тема 2.2 Эволюция моделей информационной безопасности бизнеса. Риски, рисковые события, ущербы и уязвимости

Раздел 3. Основные источники рисков в информационной сфере организации

Тема 3.1 Сложность информационной сферы

Тема 3.2 Неточность отображения материального мира в информационные модели

Тема 3.3 Управление информационной безопасностью, связанной с персоналом. Конфликт интересов

Раздел 4. Основные модели и методы управления информационной

безопасностью

Тема 4.1 Процессы управления информационной безопасностью бизнеса (деятельности) в зависимости от целей бизнеса в информационной сфере

Тема 4.2 Модели и методы измерения и оценивания информационной безопасности

Практические занятия в форме семинаров

№ п/п	Номер раздела дисциплины	Наименование практических занятий	Трудоемкость (час.)
1	1	Представление деятельности организации в информационной сфере. Бизнес-процессы, информационные активы	4
2	2	Факторы рисков информационной сферы. Риск-ориентированный подход к обеспечению информационной безопасности. Модель с изменением цели	4
3	3	Идентификация и обсуждение источников рисков в информационной сфере объекта. Деструктивное информационное воздействие	2
4	3	Факторы рисков информационной безопасности бизнеса и деятельности организации, связанные с персоналом. Факторная модель рисков информационной безопасности, связанных с персоналом	4
5	4	Объектоориентированная, рискориентированная, процессноориентированная модели оценки информационной безопасности. Модель измерения и оценивания информационной безопасности. Формирование основных, производных мер, показателей	4

5. Образовательные технологии

В ходе освоения дисциплины «Информационная безопасность бизнеса и деятельности организаций» 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 2.1, 2.2, 3.1, 3.2, 3.3, 4.1.

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 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 3.3, 4.1, 4.2

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

2.1. *Проблемные лекции*, в ходе которых используются презентации, содержащие иллюстрации приводимых положений, элементы математических моделей. В виде проблемных лекций с использованием медиатехнологий реализуется темы 2.1, 2.2, 3.1, 3.2, 3.3, 4.1.

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 1.2, 2.1, 3.1, 4.1.

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
1-4	Тема 1.1 Информационная основа бизнеса (деятельности) организации Тема 1.2 Информационные характеристики бизнеса	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Представление деятельности организации в информационной сфере. Бизнес-процессы, информационные активы»	Основная: 1 Дополнительная: 1	8
5-8	Тема 2.1 Общая структура информационной сферы. Связь с материальным миром Тема 2.2 Эволюция моделей информационной безопасности бизнеса. Риски, рисковые события, ущербы и уязвимости	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Факторы рисков информационной сферы. Риск-ориентированный подход к обеспечению информационной безопасности. Модель с изменением цели»	Основная: 1 Дополнительная: 1	8
9-12	Тема 3.1 Сложность информационной сферы организации Тема 3.2 Неточность отображения материального мира в информационные модели	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Идентификация и обсуждение источников рисков в информационной сфере объекта. Деструктивное информационное воздействие (дезинформирование, несвоевременность информации, манипулирование информацией, повышение меры хаоса в принятии решений)»	Основная: 1 Дополнительная: 1	8
13-14	Тема 3.3 Управление информационной безопасностью, связанной с персоналом. Конфликт интересов	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Факторы рисков информационной безопасности бизнеса и деятельности организации, связанные с персоналом. Факторная модель	Основная: 1 Дополнительная: 2, 3	4

			рисков информационной безопасности, связанных с персоналом»		
15-18	Тема 4.1 Процессы управления информационной безопасностью бизнеса в зависимости от целей бизнеса в информационной сфере Тема 4.2 Модели и методы измерения и оценивания информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к семинару-круглому столу «Модель измерения и оценивания информационной безопасности. Формирование основных, производных мер, показателей. Модель измерения и оценивания информационной безопасности. Формирование основных, производных мер, показателей»	Основная: 1 Дополнительная: 3,4	8

6.1.2 План самостоятельной работы аспирантов заочной формы обучения

№ сем.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Тема 1.1 Информационная основа бизнеса (деятельности) организации	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Информационный констекст бизнеса»	Основная: 1 Дополнительная: 1	6
	Тема 1.2 Информационные характеристики бизнеса	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Правовая среда бизнеса и ее свойства. Внутренняя нормативная, учредительная и лицензионная база организации. Информационная сфера – главный источник рисков бизнеса»	Основная: 1 Дополнительная: 1	6
	Тема 2.1 Общая структура информационной сферы. Связь с материальным миром	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Обобщенная модель распределения ресурсов организации в условиях рисков. Накопление знаний о событиях информационной безопасности»	Основная: 1 Дополнительная: 1	6
	Тема 2.2 Эволюция моделей информационной безопасности бизнеса. Риски, рисковые события, ущербы и уязвимости	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Риск-ориентированный подход к обеспечению информационной безопасности. Модель с изменением цели»	Основная: 1 Дополнительная: 1	8
	Тема 3.1 Сложность информационной сферы организации	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Модель организации как совокупности процессов. Управление информационной сферой»	Основная: 1 Дополнительная: 1	7
	Тема 3.2 Неточность отображения материального мира в информационные модели	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Обеспечение адекватности информационных моделей реальным объектам бизнеса. Деструктивное информационное воздействие»	Основная: 1 Дополнительная: 1	7
	Тема 3.3 Управление	Подготовка	Подготовка к лекционному	Основная: 1	8

	информационной безопасностью, связанной с персоналом. Конфликт интересов	к аудиторным занятиям	занятию по следующим вопросам «Угрозы информационной безопасности, связанные с персоналом. Модели угроз информационной безопасности, связанной с персоналом»	Дополнительная: 2, 3	
	Тема 4.1 Процессы управления информационной безопасностью бизнеса в зависимости от целей бизнеса в информационной сфере	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Влияние процессов управления информационной безопасностью на достижение целей информационной безопасности бизнеса»	Основная: 1 Дополнительная: 1, 2, 3	7
	Тема 4.2 Модели и методы измерения и оценивания информационной безопасности	Подготовка к аудиторным занятиям	Подготовка к лекционному занятию по следующим вопросам «Объектоориентированная, рискориентированная, процессноориентированная модели оценки информационной безопасности»	Основная: 1 Дополнительная: 3,4	8

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

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	Разделы 1, 2, 3, 4	ОПК-1,3 ПК-4,5,7
3	Экзамен	Разделы 1, 2, 3, 4	ОПК-1,3 ПК-4,5,7

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	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

Примерные вопросы для собеседования

Основные информационные характеристики бизнеса
Способ предварительный анализ событий информационной безопасности
Способ идентификации событий информационной безопасности
Модель организации как совокупности процессов
Виды и характеристики деструктивных информационных воздействий

Примерный перечень вопросов и заданий к экзамену

1. Информационные характеристики бизнеса (деятельности)
2. Уязвимости процессов накопления знаний
3. Общая структура информационной сферы
4. Правовая среда бизнеса и ее свойства
5. Учредительная, лицензионная и нормативная база организации
6. Отражение материального мира
7. Риски, рисковые события, ущербы и уязвимости
8. Обобщенная модель распределения ресурсов организации в условиях рисков
9. Ущербы и негативные последствия
10. Риск-ориентированный подход к обеспечению информационной безопасности
11. Модель с изменением цели
12. Идентификация событий информационной безопасности
13. Предварительный анализ событий информационной безопасности
14. Накопление знаний о событиях информационной безопасности
15. Интерпретация характеристик риска для управления информационной безопасностью
16. Общая модель обеспечения информационной безопасности бизнеса
17. Модель организации как совокупности процессов. Управление информационной сферой
18. Обеспечение адекватности целей информационной безопасности целям информационной сферы организации
19. Управление информационной безопасностью сложных изменяющихся систем
20. Деструктивное информационное воздействие (дезинформирование, манипулирование информацией, повышение меры хаоса в принятии решений)
21. Способы обеспечения достоверности информации (выбор доверенного источника, сравнение информации, полученной из разных источников, проверка целостности информации)
22. Управление информационной безопасностью сложных систем принятия решений

23. Угрозы информационной безопасности, связанные с персоналом. Модели угроз (деятельность в рамках полномочий, превышение полномочий, сговор, использование внешних связей)
24. Снижение риска информационной безопасности, связанного с персоналом (обеспечение осведомлённости об информационной безопасности, скрытность противодействия, управление системой ролей, применение аппаратно-программных средств защиты от утечки информации)
25. Управление информационной безопасностью, связанной с персоналом

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Обеспечение информационной безопасности бизнеса [Электронный ресурс] /В.В.Андрианов, С.Л.Зефиров, Н.А.Голдуев. – М.: Альпина Паблишерс, 2011. – 373с.
http://znanium.com/bookread2.php?book=556539

7.2 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
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/51406

6.3 Интернет-ресурсы

http://window.edu.ru/
http://elibrary.ru/
http://znanium.com/

8. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения лекционных, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Оснащение аудитории:
- комплект учебной мебели: парты, стол преподавательский, стулья, доска;
- мультимедийная система: проектор, экран настенный, ноутбук.

Программное обеспечение ноутбука аудитории:
- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

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	Без изменений			
2017-2018	пр-л №1 от 31.08.17	Обновлен раздел 7	12, 13		