МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы организационно-правового обеспечения информационной безопасности сетей и систем

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль): **Защищенные системы и сети связи**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **2**
Семестр: **4**
Учебный план набора 2014 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	Всего	Единицы
1	Лекции	24	24	часов
2	Практические занятия	18	18	часов
3	Лабораторные занятия	18	18	часов
4	Всего аудиторных занятий	60	60	часов
5	Самостоятельная работа	48	48	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е

Зачет: 4 семестр

Томск 2016

Согласована на портале № 6374

Рассмотрена и одобрена на заседании кафедры
протокол № 2 от « 3 » 10 2016 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.03.02 Инфокоммуникационные технологии и системы связи, утвержденного 2015-03-06 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

доцент каф. РЗИ _____ Кшнянкин А. П.

Заведующий обеспечивающей каф.
РЗИ _____ Задорин А. С.

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ Попова К. Ю.

Заведующий выпускающей каф.
РЗИ _____ Задорин А. С.

Эксперты:

Ведущий инженер каф. РЗИ _____ Зеленецкая Ю. В.

Согласована на портале № 6374

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является формирование у студентов устойчивых основ знаний организационного и правового обеспечения информационной безопасности сетей и систем , приобретения при этом необходимых знаний, умений и навыков.

1.2. Задачи дисциплины

– Основными задачами изучения дисциплины являются:

– • изучение законодательства Российской Федерации в области информационной безопасности. Виды защищаемой информации;

– • изучение системы защиты государственной тайны и конфиденциальной информации;

– • изучение основ защита интеллектуальной собственности и основ международного законодательства в области защиты информации;

– • изучение общих вопросов организационного обеспечения информационной безопасности;

– • изучение средств и методов физической защиты объектов;

– • изучение организации пропускного и внутриобъектового режимов.

– • изучение методики анализа и оценки угроз информационной безопасности объекта.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы организационно-правового обеспечения информационной безопасности сетей и систем» (Б1.В.ОД.10) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: .

Последующими дисциплинами являются: Основы информационной безопасности сетей и систем.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-8 умением собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов;

– ПК-16 готовностью изучать научно-техническую информацию, отечественный и зарубежный опыт по тематике исследования;

В результате изучения дисциплины студент должен:

– **знать** • основные законодательные и нормативные правовые документы в области защиты информации; • правовые основы организации защиты государственной тайны и конфиденциальной информации; • организационные основы обеспечения информационной безопасности сетей и систем.

– **уметь** • применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности сетей и систем.

– **владеть** • навыками организационного и правового обеспечения информационной безопасности сетей и систем

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		4 семестр
Аудиторные занятия (всего)	60	60
Лекции	24	24

Согласована на портале № 6374

Практические занятия	18	18
Лабораторные занятия	18	18
Самостоятельная работа (всего)	48	48
Оформление отчетов по лабораторным работам	19	19
Проработка лекционного материала	15	15
Подготовка к практическим занятиям, семинарам	14	14
Всего (без экзамена)	108	108
Общая трудоемкость час	108	108
Зачетные Единицы Трудоемкости	3.0	3.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

№	Названия разделов дисциплины	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	(без экзамена) Всего часов	компетенции Формируемые
1	Введение.	2	0	0	1	3	ПК-8
2	Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	3	2	3	6	14	ПК-16, ПК-8
3	Система защиты государственной тайны и конфиденциальной информации.	3	6	4	9	22	ПК-16, ПК-8
4	Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	3	2	0	3	8	ПК-16, ПК-8
5	Общие вопросы организационного обеспечения информационной безопасности.	3	2	0	3	8	ПК-16, ПК-8
6	Средства и методы физической защиты объектов.	3	2	3	7	15	ПК-8
7	Организация пропускного и внутриобъектового режимов объектов.	3	0	4	5	12	ПК-16, ПК-8
8	Методика анализа и оценки угроз информационной безопасности объекта.	4	4	4	7	19	ПК-16, ПК-8

Согласована на портале № 6374

9	Зачёт.	0	0	0	7	7	ПК-16, ПК-8
	Итого	24	18	18	48	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	ч Трудоемкость,	компетенции Формируемые
4 семестр			
1 Введение.	Цели, структура и задачи курса. Понятие организационного и правового обеспечения информационной безопасности. Взаимосвязь курса с другими дисциплинами. Специфика курса.	2	ПК-8
	Итого	2	
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Понятие права. Отрасли права, обеспечивающие законность в области защиты информации. Основные информационные права и свободы и их ограничения. Признаки охраноспособности права на информацию с ограниченным доступом. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, тайна следствия и судопроизводства, персональные данные, сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.	3	ПК-16
	Итого	3	
3 Система защиты государственной тайны и конфиденциальной информации.	Правовой режим защиты государственной тайны, закон «О государственной тайне». Организация и обеспечение режима секретности. Организационно-правовая защита служебной тайны. Закон «О коммерческой тайне». Закон «О персональных данных». Лицензирование и сертификация в	3	ПК-16, ПК-8

Согласована на портале № 6374

	области защиты информации. Правовые основы защиты информации с использованием технических средств. Система правовой ответственности за разглашение защищаемой информации и невыполнение правил ее защиты.		
	Итого	3	
4 Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	Понятие интеллектуальной собственности. Гражданский кодекс – источник норм в области защиты интеллектуальной собственности: авторское право и смежные права, патентное право, законодательство о средствах индивидуализации участников гражданского оборота. Система правовой ответственности за нарушения законодательства об интеллек-туальной собственности. Основы международного законодательства в области защиты информации. Парижская конвенция по охране промышленной собственности. Договор о патентной кооперации. Евразийская патентная конвенция.	3	ПК-16, ПК-8
	Итого	3	
5 Общие вопросы организационного обеспечения информационной безопасности.	Принципы обеспечения информационной безопасности. Взаимосвязь службы безопасности предприятия с государственными органами обеспечения безопасности. Федеральная служба безопасности. Служба специальной связи. Служба безопасности объекта. Структура службы безопасности объекта. Задачи, решаемые службой безопасности объекта.	3	ПК-16
	Итого	3	
6 Средства и методы физической защиты объектов.	Демонстративная и скрытная охрана. Охрана путем выставления постов и с помощью технических средств. Многорубежная защита. Режим охраны. Нештатные ситуации, требующие усиления режима охраны. Принцип экономичности при построении комплексной системы защиты.	3	ПК-8
	Итого	3	
7 Организация пропускного и внутриобъектового режимов объектов.	Понятия пропускного и внутриобъектового режимов. Пропускные документы.	3	ПК-8

Согласована на портале № 6374

	Удостоверения, постоянные, временные, разовые и материальные пропуска. Компьютерные системы контроля доступа. Защита информации в экстремальных ситуациях. Информационная безопасность объекта при осуществлении международного сотрудничества.		
	Итого	3	
8 Методика анализа и оценки угроз информационной безопасности объекта.	Классификация угроз информационной безопасности объекта. Внешние и внутренние угрозы. Угрозы конфиденциальности, целостности, доступности данных. Типичные каналы утечки информации. Анализ и оценка рисков. Анализ рисков без их числовых характеристик. Анализ рисков, включающий определение ценности ресурсов, оценку угроз и оценку эффективности принятых мер. Определение ценности ресурсов: физических, информационных. Оценка вероятности реализации угроз. Оценка ущерба.	4	ПК-8
	Итого	4	
Итого за семестр		24	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представ-лены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

№	Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин								
		1	2	3	4	5	6	7	8	9
Последующие дисциплины										
1	Основы информационной безопасности сетей и систем					+				

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Согласована на портале № 6374

Таблица 5. 4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий				Формы контроля
	Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа	
ПК-8	+	+	+	+	Конспект самоподготовки, Защита отчета, Компонент своевременности, Отчет по лабораторной работе, Опрос на занятиях, Зачет, Тест
ПК-16	+	+	+	+	Конспект самоподготовки, Защита отчета, Компонент своевременности, Отчет по лабораторной работе, Опрос на занятиях, Зачет, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП

7. Лабораторный практикум

Содержание лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Содержание лабораторных работ

Названия разделов	Содержание лабораторных работ	ч Трудоемкость,	компетенции Формируемые
4 семестр			
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Разработка проектов документального оформления основных видов защищаемой информации.	3	ПК-8
	Итого	3	
3 Система защиты государственной тайны и конфиденциальной информации.	Разработка проектов документального оформления основных видов конфиденциальной информации.	4	ПК-8
	Итого	4	

Согласована на портале № 6374

6 Средства и методы физической защиты объектов.	Моделирование систем физической защиты объектов.	3	ПК-8
	Итого	3	
7 Организация пропускного и внутриобъектового режимов объектов.	Практические правила обеспечения защиты объектов.	4	ПК-16, ПК-8
	Итого	4	
8 Методика анализа и оценки угроз информационной безопасности объекта.	Практика анализа и оценки угроз информационной безопасности объекта защиты.	4	ПК-16, ПК-8
	Итого	4	
Итого за семестр		18	

8. Практические занятия

Содержание практических работ приведено в таблице 8.1.

Таблица 8. 1 – Содержание практических работ

Названия разделов	Содержание практических занятий	ч Трудоемкость,	компетенции Формируемые
4 семестр			
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Общие вопросы. Право на информацию и его ограничения. Виды защищаемой информации	2	ПК-8
	Итого	2	
3 Система защиты государственной тайны и конфиденциальной информации.	Защита коммерческой тайны.	4	ПК-8
	Система правовой ответственности за разглашение защищаемой информации и невыполнение правил ее защиты	2	
	Итого	6	
4 Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	Организационно-правовая защита служебной тайны.	2	ПК-8
	Итого	2	
5 Общие вопросы организационного обеспечения информационной безопасности.	Служба безопасности объекта.	2	ПК-8
	Итого	2	
6 Средства и методы физической защиты объектов.	Средства и методы физической защиты объектов. Организация пропускного и внутриобъектового режимов	2	ПК-8
	Итого	2	

Согласована на портале № 6374

8 Методика анализа и оценки угроз информационной безопасности объекта.	Анализ и оценка угроз информационной безопасности объекта.	4	ПК-8
	Итого	4	
Итого за семестр		18	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	ч Трудоемкость	компетенции Формируемые	Формы контроля
4 семестр				
1 Введение.	Проработка лекционного материала	1	ПК-8	Зачет, Конспект самоподготовки, Опрос на занятиях
	Итого	1		
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Подготовка к практическим занятиям, семинарам	2	ПК-8, ПК-16	Зачет, Защита отчета, Компонент своевременности, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	3		
	Итого	6		
3 Система защиты государственной тайны и конфиденциальной информации.	Подготовка к практическим занятиям, семинарам	2	ПК-16, ПК-8	Зачет, Защита отчета, Компонент своевременности, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Подготовка к практическим занятиям, семинарам	2		
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
4 Основы защиты интеллектуальной собственности и основ международного	Подготовка к практическим занятиям, семинарам	2	ПК-8, ПК-16	Зачет, Компонент своевременности, Конспект самоподготовки, Опрос
	Проработка лекционного	1		

Согласована на портале № 6374

законодательства в области защиты информации.	материала			на занятиях, Тест
	Итого	3		
5 Общие вопросы организационного обеспечения информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ПК-8, ПК-16	Зачет, Компонент своевременности, Конспект самоподготовки, Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Итого	3		
6 Средства и методы физической защиты объектов.	Подготовка к практическим занятиям, семинарам	2	ПК-8	Зачет, Защита отчета, Компонент своевременности, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	7		
7 Организация пропускного и внутриобъектового режимов объектов.	Проработка лекционного материала	1	ПК-8, ПК-16	Зачет, Защита отчета, Компонент своевременности, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	4		
	Итого	5		
8 Методика анализа и оценки угроз информационной безопасности объекта.	Подготовка к практическим занятиям, семинарам	2	ПК-8	Зачет, Защита отчета, Компонент своевременности, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	7		
9 Зачёт.	Проработка лекционного материала	7	ПК-16, ПК-8	Зачет
	Итого	7		
Итого за семестр		48		
Итого		48		

9.1. Вопросы на проработку лекционного материала

1. - Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.
2. - Система защиты государственной тайны и конфиденциальной информации.
3. - Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.
4. - Общие вопросы организационного обеспечения информационной безопасности.
5. - Средства и методы физической защиты объектов.
6. - Организация пропускного и внутриобъектового режимов объектов.
7. - Методика анализа и оценки угроз информационной безопасности объекта.

Согласована на портале № 6374

10. Курсовая работа

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Бальные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
4 семестр				
Зачет	8	10	11	29
Защита отчета	3	3	3	9
Компонент своевременности	4	4	4	12
Конспект самоподготовки	4	4	4	12
Опрос на занятиях	4	4	6	14
Отчет по лабораторной работе	3	3	3	9
Тест	5	5	5	15
Итого максимум за период	31	33	36	100
Нарастающим итогом	31	64	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	

Согласована на портале № 6374

	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Защита прав интеллектуальной собственности: Учебное пособие / Сычев А. Н. - 2014. 240 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/4967, свободный.
2. Государственная и муниципальная служба РФ: Учебное пособие для бакалавров / Грик Н. А. - 2016. 97 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/6121, свободный.

12.2. Дополнительная литература

1. Документирование управленческой деятельности: Учебное пособие / Аксёнова Ж. Н. - 2009. 194 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/4875, свободный.

12.3. Учебно-методическое пособие и программное обеспечение

1. Организационное обеспечение информационной безопасности: Методические указания для практических занятий / Белицкая Л. А. - 2011. 22 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/3030, свободный.
2. Организационно-правовое обеспечение информационной безопасности: Методические указания по практическим занятиям и самостоятельной работе / Семенов Э. В. - 2012. 13 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/2506, свободный.
3. Защита и обработка конфиденциальных документов: Методические указания для практических занятий / Белицкая Л. А. - 2011. 56 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/3031, свободный.
4. Моделирование и анализ бизнес-процессов. Часть I: Методические указания для выполнения лабораторных работ по дисциплине для студентов направления "Программная инженерия" / Силич М. П. - 2014. 72 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/6457, свободный.

12.4. Базы данных, информационно справочные и поисковые системы

1. 1. Базовые законодательные и нормативно-правовые документы РФ в области защиты информации.
2. [Электронный ресурс]. - Режим доступа: http://www.consultant.ru, (дата обращения 31.10.2016);
3. 2. Научно-образовательный портал ТУСУРа, https://edu.tusur.ru

13. Материально-техническое обеспечение дисциплины

Лекционные, практические и лабораторные занятия проводятся в специализированных аудиториях кафедры РЗИ.

14. Фонд оценочных средств

Фонд оценочных средств приведен в приложении 1.

15. Методические рекомендации по организации изучения дисциплины

Без рекомендаций.

Согласована на портале № 6374

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Основы организационно-правового обеспечения информационной безопасности сетей и систем

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль): **Защищенные системы и сети связи**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **2**
Семестр: **4**

Учебный план набора 2014 года

Разработчики:

- доцент каф. РЗИ Кшнянкин А. П.

Зачет: 4 семестр

Томск 2016

Согласована на портале № 6374

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПК-8	умением собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов	Должен знать • основные законодательные и нормативные правовые документы в области защиты информации; • правовые основы организации защиты государственной тайны и конфиденциальной информации; • организационные основы обеспечения информационной безопасности сетей и систем. ; Должен уметь • применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности сетей и систем.; Должен владеть • навыками организационного и правового обеспечения информационной безопасности сетей и систем ;
ПК-16	готовностью изучать научно-техническую информацию, отечественный и зарубежный опыт по тематике исследования	

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

Согласована на портале № 6374

2 Реализация компетенций

2.1 Компетенция ПК-8

ПК-8: умением собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	• Основные законодательные и нормативные правовые документы в области защиты информации в полном объеме курса; • Правовые основы организации защиты государственной тайны и конфиденциальной информации в полном объеме курса; • Организационные основы обеспечения информационной безопасности сетей и систем в полном объеме курса	Применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности сетей и систем.	Навыками организационного и правового обеспечения информационной безопасности сетей и систем.
Виды занятий	• Практические занятия; • Лабораторные занятия; • Лекции; • Самостоятельная работа;	• Практические занятия; • Лабораторные занятия; • Лекции; • Самостоятельная работа;	• Лабораторные занятия; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Конспект самоподготовки; • Тест; • Зачет;	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Конспект самоподготовки; • Тест; • Зачет;	• Отчет по лабораторной работе; • Зачет; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• основные законодательные и нормативные правовые документы в области защиты информации в	• применять законодательную и нормативно-правовую базу в области защиты информации для	• навыками организационного и правового обеспечения информационной безопасности сетей и

Согласована на портале № 6374

	полном объеме курса; ; • правовые основы организации защиты государственной тайны и конфиденциальной информации в полном объеме курса; ; • организационные основы обеспечения информационной безопасности сетей и систем в полном объеме курса;	организационного и правового обеспечения информационной безопасности сетей и систем в полном объеме курса;	систем в полном объеме курса;
Хорошо (базовый уровень)	• основные законодательные и нормативные правовые документы в области защиты информации с незначительным ошибками; ; • правовые основы организации защиты государственной тайны и конфиденциальной информации с незначительным ошибками ; • организационные основы обеспечения информационной безопасности сетей и систем с незначительным ошибками;	• применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности сетей и систем с незначительными ошибками;	• навыками организационного и правового обеспечения информационной безопасности сетей и систем с незначительными ошибками;
Удовлетворительно (пороговый уровень)	• основные законодательные и нормативные правовые документы в области защиты информации с существенными ошибками; ; • правовые основы организации защиты государственной тайны и конфиденциальной информации с существенными ошибками;; • организационные основы обеспечения информационной безопасности сетей и систем с	• применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности сетей и систем с существенными ошибками;	• навыками организационного и правового обеспечения информационной безопасности сетей и систем с существенными ошибками;

Согласована на портале № 6374

	существенными ошибками;		

2.2 Компетенция ПК-16

ПК-16: готовностью изучать научно-техническую информацию, отечественный и зарубежный опыт по тематике исследования.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	• Основные законодательные и нормативные правовые документы в области защиты информации; • Правовые основы организации защиты государственной тайны и конфиденциальной информации; • Организационные основы обеспечения информационной безопасности сетей и систем.	Применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности сетей и систем.	• Навыками организационного и правового обеспечения информационной безопасности сетей и систем
Виды занятий	• Практические занятия; • Лабораторные занятия; • Лекции; • Самостоятельная работа;	• Практические занятия; • Лабораторные занятия; • Лекции; • Самостоятельная работа;	• Лабораторные занятия; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Конспект самоподготовки; • Тест; • Зачет;	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Конспект самоподготовки; • Тест; • Зачет;	• Отчет по лабораторной работе; • Зачет; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• основные законодательные и нормативные правовые документы в области защиты информации в полном объеме курса; ;	• применять законодательную и нормативно-правовую базу в области защиты информации для организационного и	• навыками организационного и правового обеспечения информационной безопасности сетей и систем в полном объеме

Согласована на портале № 6374

	• правовые основы организации защиты государственной тайны и конфиденциальной информации в полном объеме курса; ; • организационные основы обеспечения информационной безопасности сетей и систем в полном объеме курса ;	правового обеспечения информационной безопасности сетей и систем в полном объеме курса;	курса ;
Хорошо (базовый уровень)	• основные законодательные и нормативные правовые документы в области защиты информации с незначительными ошибками; ; • правовые основы организации защиты государственной тайны и конфиденциальной информации с незначительными ошибками;; • организационные основы обеспечения информационной безопасности сетей и систем с незначительными ошибками;	• применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности сетей и систем с незначительными ошибками;	• навыками организационного и правового обеспечения информационной безопасности сетей и систем с незначительными ошибками;
Удовлетворительно (пороговый уровень)	• основные законодательные и нормативные правовые документы в области защиты информации с существенными ошибками; ; • правовые основы организации защиты государственной тайны и конфиденциальной информации с существенными ошибками;; • организационные основы обеспечения информационной безопасности сетей и систем с существенными	• применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности сетей и систем с существенными ошибками;	• навыками организационного и правового обеспечения информационной безопасности сетей и систем с существенными ошибками;

Согласована на портале № 6374

	ошибками;		

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Вопросы на самоподготовку

- Право на информацию и его ограничения. Виды защищаемой информации.
- Система защиты государственной тайны и конфиденциальной информации.
- Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.
- Общие вопросы организационного обеспечения информационной безопасности.
- Средства и методы физической защиты объектов.
- Методика анализа и оценки угроз информационной безопасности объекта.

3.2 Тестовые задания

- • Что составляет основу законодательной и нормативно-правовой базы государственной системы защиты информации.
- • Дать определение и понятие защищаемой информации, конфиденциальной информации
- • Основные законодательные акты, регулирующие ограничение доступа к информации.
- • Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.
- • Общие вопросы организационного обеспечения информационной безопасности.
- • Средства и методы физической защиты объектов.
- • Организация пропускного и внутриобъектового режимов объектов.
- • Методика анализа и оценки угроз информационной безопасности объекта.

3.3 Зачёт

- - Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.
- - Система защиты государственной тайны и конфиденциальной информации.
- - Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.
- - Общие вопросы организационного обеспечения информационной безопасности.
- - Средства и методы физической защиты объектов.
- - Организация пропускного и внутриобъектового режимов объектов.
- - Методика анализа и оценки угроз информационной безопасности объекта.

3.4 Темы опросов на занятиях

- Цели, структура и задачи курса. Понятие организационного и правового обеспечения информационной безопасности. Взаимосвязь курса с другими дисциплинами. Специфика курса.
- Понятие права. Отрасли права, обеспечивающие законность в области защиты информации. Основные информационные права и свободы и их ограничения. Признаки охраноспособности права на информацию с ограниченным доступом. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, тайна следствия и судопроизводства, персональные данные, сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.
- Правовой режим защиты государственной тайны, закон «О государственной тайне». Организация и обеспечение режима секретности. Организационно-правовая защита служебной тайны. Закон «О коммерческой тайне». Закон «О персональных данных». Лицензирование и сертификация в области защиты информации. Правовые основы защиты информации с

Согласована на портале № 6374

использованием технических средств. Система правовой ответственности за разглашение защищаемой информации и невыполнение правил ее защиты.

– Понятие интеллектуальной собственности. Гражданский кодекс – источник норм в области защиты интеллектуальной собственности: авторское право и смежные права, патентное право, законодательство о средствах индивидуализации участников гражданского оборота. Система правовой ответственности за нарушения законодательства об интеллек-туальной собственности. Основы международного законодательства в области защиты информации. Парижская конвенция по охране промышленной собственности. Договор о патентной кооперации. Евразийская патентная конвенция.

– Принципы обеспечения информационной безопасности. Взаимосвязь службы безопасности предприятия с государственными органами обеспечения безопасности. Федеральная служба безопасности. Служба специальной связи. Служба безопасности объекта. Структура службы безопасности объекта. Задачи, решаемые службой безопасности объекта.

– Демонстративная и скрытная охрана. Охрана путем выставления постов и с помощью технических средств. Многорубежная защита. Режим охраны. Нештатные ситуации, требующие усиления режима охраны. Принцип экономичности при построении комплексной системы защиты.

– Понятия пропускного и внутриобъектового режимов. Пропускные документы. Удостоверения, постоянные, временные, разовые и материальные пропуска. Компьютерные системы контроля доступа. Защита информации в экстремальных ситуациях. Информационная безопасность объекта при осуществлении международного сотрудничества.

– Классификация угроз информационной безопасности объекта. Внешние и внутренние угрозы. Угрозы конфиденциальности, целостности, доступности данных. Типичные каналы утечки информации. Анализ и оценка рисков. Анализ рисков без их числовых характеристик. Анализ рисков, включающий определение ценности ресурсов, оценку угроз и оценку эффективности принятых мер. Определение ценности ресурсов: физических, информационных. Оценка вероятности реализации угроз. Оценка ущерба.

3.5 Темы лабораторных работ

– Разработка проектов документального оформления основных видов защищаемой информации.

– Разработка проектов документального оформления основных видов конфиденциальной информации.

– Моделирование систем физической защиты объектов.

– Практические правила обеспечения защиты объектов.

– Практика анализа и оценки угроз информационной безопасности объекта защиты.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Защита прав интеллектуальной собственности: Учебное пособие / Сычев А. Н. - 2014. 240 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/4967, свободный.

2. Государственная и муниципальная служба РФ: Учебное пособие для бакалавров / Грик Н. А. - 2016. 97 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/6121, свободный.

4.2. Дополнительная литература

1. Документирование управленческой деятельности: Учебное пособие / Аксёнова Ж. Н. - 2009. 194 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/4875, свободный.

4.3. Учебно-методическое пособие и программное обеспечение

1. Организационное обеспечение информационной безопасности: Методические указания

Согласована на портале № 6374

для практических занятий / Белицкая Л. А. - 2011. 22 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/3030, свободный.

2. Организационно-правовое обеспечение информационной безопасности: Методические указания по практическим занятиям и самостоятельной работе / Семенов Э. В. - 2012. 13 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/2506, свободный.

3. Защита и обработка конфиденциальных документов: Методические указания для практических занятий / Белицкая Л. А. - 2011. 56 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/3031, свободный.

4. Моделирование и анализ бизнес-процессов. Часть I: Методические указания для выполнения лабораторных работ по дисциплине для студентов направления "Программная инженерия" / Силич М. П. - 2014. 72 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/6457, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. 1. Базовые законодательные и нормативно-правовые документы РФ в области защиты информации.

2. [Электронный ресурс]. - Режим доступа: http://www.consultant.ru, (дата обращения 31.10.2016);

3. 2. Научно-образовательный портал ТУСУРа, https://edu.tusur.ru

Согласована на портале № 6374