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

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **3**
Семестр: **5, 6**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	6 семестр	Всего	Единицы
1	Лекции	16	16	32	часов
2	Практические занятия	24	24	48	часов
3	Всего аудиторных занятий	40	40	80	часов
4	Из них в интерактивной форме	9	11	20	часов
5	Самостоятельная работа	32	32	64	часов
6	Всего (без экзамена)	72	72	144	часов
7	Подготовка и сдача экзамена	36		36	часов
8	Общая трудоемкость	108	72	180	часов
		3.0	2.0	5.0	З.Е

Экзамен: 5 семестр
Зачет: 6 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 5 от «28» 3 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент каф. РЗИ _____ А. П. Кшнянкин

Заведующий обеспечивающей каф.
РЗИ _____ А. С. Задорин

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

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф.
РЗИ _____ А. С. Задорин

Эксперт:

Ведущий инженер каф. РЗИ _____ Ю. В. Зеленецкая

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 объектов защиты , 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 «Организационное и правовое обеспечение информационной безопасности» (Б1.Б.18) относится к блоку 1 (базовая часть).

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

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты;

– ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

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 телекоммуникационных систем.

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

– **владеть** • навыками организационного и правового обеспечения информационной безопасности объектов защиты.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 5.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		5 семестр	6 семестр
Аудиторные занятия (всего)	80	40	40
Лекции	32	16	16
Практические занятия	48	24	24

Из них в интерактивной форме	20	9	11
Самостоятельная работа (всего)	64	32	32
Проработка лекционного материала	26	14	12
Подготовка к практическим занятиям, семинарам	38	18	20
Всего (без экзамена)	144	72	72
Подготовка и сдача экзамена	36	36	
Общая трудоемкость ч	180	108	72
Зачетные Единицы	5.0	3.0	2.0

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	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
5 семестр					
1 Введение.	2	0	3	5	ПК-3, ПК-4
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	6	8	7	21	ПК-3, ПК-4
3 Система защиты государственной тайны и конфиденциальной информации.	4	8	7	19	ПК-3, ПК-4
4 Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	4	8	7	19	ПК-3, ПК-4
5 Экзамен.	0	0	8	8	ПК-3, ПК-4
Итого за семестр	16	24	32	72	
6 семестр					
6 Общие вопросы организационного обеспечения информационной безопасности.	4	8	8	20	ПК-3, ПК-4
7 Средства и методы физической защиты объектов.	4	8	8	20	ПК-3, ПК-4
8 Организация пропускного и внутриобъектового режимов объектов.	4	0	6	10	ПК-3, ПК-4
9 Методика анализа и оценки угроз информационной безопасности объекта.	4	8	10	22	ПК-3, ПК-4
10 Зачет.	0	0	0	0	

Итого за семестр	16	24	32	72	
Итого	32	48	64	144	

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	Трудоемкость, ч	Формируемые компетенции
5 семестр			
1 Введение.	Цели, структура и задачи курса. Понятие организационного и правового обеспечения информационной безопасности. Взаимосвязь курса с другими дисциплинами. Специфика курса.	2	ПК-3, ПК-4
	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.	6	ПК-3, ПК-4
	Итого	6	
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 области защиты информации. Правовые основы защиты информации с использованием технических средств. Система правовой ответственности за разглашение защищаемой информации и невыполнение правил ее защиты.	4	ПК-3, ПК-4
	Итого	4	
4 Основы защиты	Понятие интеллектуальной собствен-	4	ПК-3, ПК-

интеллектуальной собственности и основ международного законодательства в области защиты информации.	ности. 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.		4
	Итого	4	
Итого за семестр		16	
6 семестр			
6 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.	4	ПК-3, ПК-4
	Итого	4	
7 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.	4	ПК-3, ПК-4
	Итого	4	
8 Организация пропускного и внутриобъектового режимов объектов.	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.	4	ПК-3, ПК-4
	Итого	4	
9 Методика анализа и оценки угроз	Классификация угроз информацион-	4	ПК-3, ПК-

информационной безопасности объекта.	ной 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
	Итого	4	
Итого за семестр		16	
Итого		32	

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 представлены 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	10
Предшествующие дисциплины										
1 Информатика	+	+								

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

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий			Формы контроля
	Лекции	Практические занятия	Самостоятельная работа	
ПК-3	+	+	+	Экзамен, Конспект самоподготовки, Опрос на занятиях, Зачет
ПК-4	+	+	+	Экзамен, Конспект самоподготовки, Опрос на занятиях, Зачет

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лекции	Всего
5 семестр			
Мозговой штурм	2	1	3
Решение ситуационных задач	2	1	3
Презентации с использованием слайдов с обсуждением	1	2	3
Итого за семестр:	5	4	9
6 семестр			
Мозговой штурм	2	2	4
Решение ситуационных задач	3	1	4
Презентации с использованием слайдов с обсуждением	2	1	3
Итого за семестр:	7	4	11
Итого	12	8	20

7. Лабораторные работы

Не предусмотрено РУП

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
5 семестр			
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Общие вопросы. Право на информацию и его ограничения. Виды защищаемой информации	8	ПК-3, ПК-4
	Итого	8	
3 Система защиты государственной тайны и конфиденциальной информации.	Защита коммерческой тайны.	4	ПК-3, ПК-4
	Система правовой ответственности за разглашение защищаемой информации и невыполнение правил ее защиты	4	
	Итого	8	
4 Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	Организационно-правовая защита служебной тайны.	8	ПК-3, ПК-4
	Итого	8	
Итого за семестр		24	
6 семестр			
6 Общие вопросы	Служба безопасности объекта.	8	ПК-3, ПК-

организационного обеспечения информационной безопасности.	Итого	8	4
7 Средства и методы физической защиты объектов.	Средства и методы физической защиты объектов. Организация пропускного и внутриобъектового режимов.	8	ПК-3, ПК-4
	Итого	8	
9 Методика анализа и оценки угроз информационной безопасности объекта.	Анализ и оценка угроз информационной безопасности объекта.	8	ПК-3, ПК-4
	Итого	8	
Итого за семестр		24	
Итого		48	

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	Трудоемкость, ч	Формируемые компетенции	Формы контроля
5 семестр				
1 Введение.	Проработка лекционного материала	3	ПК-3, ПК-4	Конспект самоподготовки, Опрос на занятиях, Экзамен
	Итого	3		
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Подготовка к практическим занятиям, семинарам	6	ПК-3, ПК-4	Конспект самоподготовки, Опрос на занятиях, Экзамен
	Проработка лекционного материала	1		
	Итого	7		
3 Система защиты государственной тайны и конфиденциальной информации.	Подготовка к практическим занятиям, семинарам	6	ПК-3, ПК-4	Конспект самоподготовки, Опрос на занятиях, Экзамен
	Проработка лекционного материала	1		
	Итого	7		
4 Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	Подготовка к практическим занятиям, семинарам	6	ПК-3, ПК-4	Конспект самоподготовки, Опрос на занятиях, Экзамен
	Проработка лекционного материала	1		
	Итого	7		
5 Экзамен.	Проработка лекционного материала	8	ПК-3, ПК-4	Экзамен

	Итого	8		
Итого за семестр		32		
	Подготовка и сдача экзамена	36		Экзамен
6 семестр				
6 Общие вопросы организационного обеспечения информационной безопасности.	Подготовка к практическим занятиям, семинарам	6	ПК-3, ПК-4	Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	2		
	Итого	8		
7 Средства и методы физической защиты объектов.	Подготовка к практическим занятиям, семинарам	6	ПК-3, ПК-4	Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	2		
	Итого	8		
8 Организация пропускного и внутриобъектового режимов объектов.	Проработка лекционного материала	6	ПК-3, ПК-4	Зачет, Конспект самоподготовки, Опрос на занятиях
	Итого	6		
9 Методика анализа и оценки угроз информационной безопасности объекта.	Подготовка к практическим занятиям, семинарам	8	ПК-3, ПК-4	Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	2		
	Итого	10		
Итого за семестр		32		
Итого		100		

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.

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с	Максимальный балл за период	Максимальный балл за период	Всего за семестр

	начала семестра	между 1КТ и 2КТ	между 2КТ и на конец семестра	
5 семестр				
Конспект самоподготовки	10	10	15	35
Опрос на занятиях	10	10	15	35
Итого максимум за период	20	20	30	70
Экзамен				30
Нарастающим итогом	20	40	70	100
6 семестр				
Зачет	10	10	20	40
Конспект самоподготовки	5	10	15	30
Опрос на занятиях	5	10	15	30
Итого максимум за период	20	30	50	100
Нарастающим итогом	20	50	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	
	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, дата обращения: 25.04.2017.
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, дата обращения: 25.04.2017.

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, дата обращения: 25.04.2017.

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

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, дата обращения: 25.04.2017.
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, дата обращения: 25.04.2017.
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, дата обращения: 25.04.2017.

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

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

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Лекционные, практические и лабораторные занятия проводятся в специализированных аудиториях кафедры РЗИ. Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной

мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебные аудитории, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 407, 412, 416. Состав оборудования: Учебная мебель; Доска магнитно-маркерная -1шт.; Коммутатор D-Link Switch 24 port - 1шт.; Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. -14 шт. Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3/Microsoft Windows 7 Professional with SP1; Microsoft Windows Server 2008 R2; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft Office Access 2003; VirtualBox 6.2. Имеется помещения для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 4 этаж, ауд. 407,412, 416. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями	Собеседование по вопросам к зачету,	Преимущественно устная проверка

зрения	опрос по терминам	(индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

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

Организационное и правовое обеспечение информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **3**
Семестр: **5, 6**

Учебный план набора 2013 года

Разработчик:
- доцент каф. РЗИ А. П. Кшнянкин

Экзамен: 5 семестр
Зачет: 6 семестр

Томск 2017

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-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	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 телекоммуникационных систем. ; Должен уметь • применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности объектов защиты.; Должен владеть • навыками организационного и правового обеспечения информационной безопасности объектов защиты. ;
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты	

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

2 Реализация компетенций

2.1 Компетенция ПК-4

ПК-4: способностью участвовать в работах по реализации политики информационной без-

опасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

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; • правовые основы организации защиты государственной тайны и конфиденциальной информации; • организационные основы обеспечения информационной безопасности объектов защиты.	• применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности объектов защиты.	• навыками организационного и правового обеспечения информационной безопасности объектов защиты.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Конспект самоподготовки; • Опрос на занятиях; • Экзамен; • Зачет;	• Конспект самоподготовки; • Опрос на занятиях; • Экзамен; • Зачет;	• Экзамен; • 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)	• 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.;

2.2 Компетенция ПК-3

ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты.

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 объектов защиты.	• применять законодательную и нормативно-правовую базу в области защиты информации для организационного и правового обеспечения информационной безопасности объектов защиты.	• навыками организационного и правового обеспечения информационной безопасности объектов защиты.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Конспект самоподготовки; • Опрос на занятиях; • Экзамен; • Зачет;	• Конспект самоподготовки; • Опрос на занятиях; • Экзамен; • Зачет;	• Экзамен; • 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)	• 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	• Обладает диапазоном практических умений,	• Берет ответственность за завершение за-

	понятия в пределах изучаемой области.;	требуемых для решения определенных проблем в области исследования. ;	дач 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.;

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 Зачёт

- •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.

3.3 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 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.

3.4 Экзаменационные вопросы

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

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. Обязательные учебно-методические пособия

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. [Элек-

тронный 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.

4.4. 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