МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования

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 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) / специализация: **Защищенные системы и сети связи**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РСС, Кафедра радиоэлектроники и систем связи**
Курс: **2**
Семестр: **4**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	Всего	Единицы
1	Лекции	40	40	часов
2	Практические занятия	34	34	часов
3	Лабораторные работы	34	34	часов
4	Всего аудиторных занятий	108	108	часов
5	Самостоятельная работа	108	108	часов
6	Всего (без экзамена)	216	216	часов
7	Общая трудоемкость	216	216	часов
		6.0	6.0	З.Е.

Дифференцированный зачет: 4 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 11 от « 3 » 7 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины 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 06.03.2015 года, рассмотрена и одобрена на заседании кафедры РСС «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент каф. РСС	_____	А. И. Кураленко
Заведующий обеспечивающей каф. РСС	_____	А. В. Фатеев

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РТФ	_____	К. Ю. Попова
Заведующий выпускающей каф. РСС	_____	А. В. Фатеев

Эксперты:

Профессор кафедры радиоэлектроники и систем связи (РСС)	_____	А. С. Задорин
Заведующий кафедрой радиоэлектроники и систем связи (РСС)	_____	А. В. Фатеев

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.ДВ.1.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Введение в профиль "Защищенные системы связи", Информатика.

Последующими дисциплинами являются: Защита информационных процессов в сетях и системах связи, Комплексные системы защиты информации в сетях и системах связи, Организация и управление службой защиты информации на предприятиях связи.

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 обучающийся 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 6.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		4 семестр
Аудиторные занятия (всего)	108	108

Лекции	40	40
Практические занятия	34	34
Лабораторные работы	34	34
Самостоятельная работа (всего)	108	108
Оформление отчетов по лабораторным работам	25	25
Проработка лекционного материала	56	56
Подготовка к практическим занятиям, семинарам	27	27
Всего (без экзамена)	216	216
Общая трудоемкость, ч	216	216
Зачетные Единицы	6.0	6.0

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	Лек., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
4 семестр						
1 Введение.	4	0	0	5	9	ПК-8
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	10	4	5	11	30	ПК-16, ПК-8
3 Система защиты государственной тайны и конфиденциальной информации.	7	12	8	19	46	ПК-16, ПК-8
4 Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	3	5	0	8	16	ПК-16, ПК-8
5 Общие вопросы организационного обеспечения информационной безопасности.	3	4	0	10	17	ПК-16, ПК-8
6 Средства и методы физической защиты объектов.	3	4	7	12	26	ПК-8
7 Организация пропускного и внутриобъектового режимов объектов.	3	0	6	9	18	ПК-16, ПК-8
8 Методика анализа и оценки угроз информационной безопасности объекта.	7	5	8	21	41	ПК-16, ПК-8
9 Дифференцированный зачет	0	0	0	13	13	ПК-16, ПК-8
Итого за семестр	40	34	34	108	216	
Итого	40	34	34	108	216	

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
4 семестр			
1 Введение.	Цели, структура и задачи курса. Понятие организационного и правового обеспечения информационной безопасности. Взаимосвязь курса с другими дисциплинами. Специфика курса.	4	ПК-8
	Итого	4	
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.	10	ПК-16
	Итого	10	
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.	7	ПК-16, ПК-8
	Итого	7	
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 патент-	3	ПК-16, ПК-8

	ной кооперации. Евразийская патентная конвенция.		
	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. Удостоверения, постоянные, временные, разовые и материальные пропуска. Компьютерные системы контроля доступа. Защита информации в экстремальных ситуациях. Информационная безопасность объекта при осуществлении международного сотрудничества.	3	ПК-8
	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.	7	ПК-8
	Итого	7	
Итого за семестр		40	

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

Предшествующие дисциплины									
1 Введение в профиль "Защищенные системы связи"		+							
2 Информатика					+				
Последующие дисциплины									
1 Защита информационных процессов в сетях и системах связи		+						+	
2 Комплексные системы защиты информации в сетях и системах связи		+			+				
3 Организация и управление службой защиты информации на предприятиях связи		+	+						

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, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	
ПК-8	+	+	+	+	Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Тест, Дифференцированный зачет
ПК-16	+	+	+	+	Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Тест, Дифференцированный зачет

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
4 семестр			

2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Разработка проектов документального оформления основных видов защищаемой информации.	5	ПК-8
	Итого	5	
3 Система защиты государственной тайны и конфиденциальной информации.	Разработка проектов документального оформления основных видов конфиденциальной информации.	8	ПК-8
	Итого	8	
6 Средства и методы физической защиты объектов.	Моделирование систем физической защиты объектов.	7	ПК-8
	Итого	7	
7 Организация пропускного и внутриобъектового режимов объектов.	Практические правила обеспечения защиты объектов.	6	ПК-16, ПК-8
	Итого	6	
8 Методика анализа и оценки угроз информационной безопасности объекта.	Практика анализа и оценки угроз информационной безопасности объекта защиты.	8	ПК-16, ПК-8
	Итого	8	
Итого за семестр		34	

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
4 семестр			
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Общие вопросы. Право на информацию и его ограничения. Виды защищаемой информации	4	ПК-8
	Итого	4	
3 Система защиты государственной тайны и конфиденциальной информации.	Защита коммерческой тайны.	6	ПК-8
	Система правовой ответственности за разглашение защищаемой информации и невыполнение правил ее защиты	6	
	Итого	12	
4 Основы защиты интеллектуальной собственности и основ	Организационно-правовая защита служебной тайны.	5	ПК-8
	Итого	5	

международного законодательства в области защиты информации.			
5 Общие вопросы организационного обеспечения информационной безопасности.	Служба безопасности объекта.	4	ПК-8
	Итого	4	
6 Средства и методы физической защиты объектов.	Средства и методы физической защиты объектов. Организация пропускного и внутриобъектового режимов	4	ПК-8
	Итого	4	
8 Методика анализа и оценки угроз информационной безопасности объекта.	Анализ и оценка угроз информационной безопасности объекта.	5	ПК-8
	Итого	5	
Итого за семестр		34	

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
4 семестр				
1 Введение.	Проработка лекционного материала	5	ПК-8	Дифференцированный зачет, Конспект самоподготовки, Опрос на занятиях, Тест
	Итого	5		
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Проработка лекционного материала	6	ПК-16, ПК-8	Защита отчета, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	5		
	Итого	11		
3 Система защиты государственной тайны и конфиденциальной информации.	Подготовка к практическим занятиям, семинарам	5	ПК-16, ПК-8	Дифференцированный зачет, Защита отчета, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Подготовка к практическим занятиям, семинарам	5		
	Проработка лекционного материала	5		
	Оформление отчетов по	4		

	лабораторным работам			
	Итого	19		
4 Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	Подготовка к практическим занятиям, семинарам	2	ПК-8, ПК-16	Дифференцированный зачет, Конспект самоподготовки, Опрос на занятиях, Тест
	Проработка лекционного материала	6		
	Итого	8		
5 Общие вопросы организационного обеспечения информационной безопасности.	Подготовка к практическим занятиям, семинарам	5	ПК-8, ПК-16	Конспект самоподготовки, Опрос на занятиях, Тест
	Проработка лекционного материала	5		
	Итого	10		
6 Средства и методы физической защиты объектов.	Подготовка к практическим занятиям, семинарам	4	ПК-8	Защита отчета, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Проработка лекционного материала	4		
	Оформление отчетов по лабораторным работам	4		
	Итого	12		
7 Организация пропускного и внутриобъектового режимов объектов.	Проработка лекционного материала	5	ПК-8, ПК-16	Дифференцированный зачет, Защита отчета, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
8 Методика анализа и оценки угроз информационной безопасности объекта.	Подготовка к практическим занятиям, семинарам	6	ПК-8	Защита отчета, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Проработка лекционного материала	7		
	Оформление отчетов по лабораторным работам	8		
	Итого	21		
9 Дифференцированный зачет	Проработка лекционного материала	13	ПК-16, ПК-8	Дифференцированный зачет, Тест
	Итого	13		
Итого за семестр		108		
Итого		108		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

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 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				
Дифференцированный зачет	7	10	10	27
Защита отчета	5	5	5	15
Конспект самоподготовки	4	4	4	12
Опрос на занятиях	4	4	6	14
Отчет по лабораторной работе	5	5	5	15
Тест	5	5	7	17
Итого максимум за период	30	33	37	100
Нарастающим итогом	30	63	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 [Электронный ресурс]: Учебное пособие / Сычев А. Н. - 2014. 240 с. - Режим доступа: http://edu.tusur.ru/publications/4967 (дата обращения: 24.07.2018).
2. Государственная и муниципальная служба РФ [Электронный ресурс]: Учебное пособие для бакалавров / Грик Н. А. - 2016. 97 с. - Режим доступа: http://edu.tusur.ru/publications/6121 (дата обращения: 24.07.2018).

12.2. Дополнительная литература

1. Документирование управленческой деятельности [Электронный ресурс]: Учебное пособие / Аксёнова Ж. Н. - 2009. 194 с. - Режим доступа: http://edu.tusur.ru/publications/4875 (дата обращения: 24.07.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Организационное обеспечение информационной безопасности [Электронный ресурс]: Методические указания для практических занятий / Белицкая Л. А. - 2011. 22 с. - Режим доступа: http://edu.tusur.ru/publications/3030 (дата обращения: 24.07.2018).
2. Организационно-правовое обеспечение информационной безопасности [Электронный ресурс]: Методические указания по практическим занятиям и самостоятельной работе / Семенов Э. В. - 2012. 13 с. - Режим доступа: http://edu.tusur.ru/publications/2506 (дата обращения: 24.07.2018).
3. Защита и обработка конфиденциальных документов [Электронный ресурс]: Методические указания для практических занятий / Белицкая Л. А. - 2011. 56 с. - Режим доступа: http://edu.tusur.ru/publications/3031 (дата обращения: 24.07.2018).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и 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. Профессиональные базы данных и информационные справочные системы

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

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

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 демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Учебная лаборатория радиоэлектроники / Лаборатория ГПО

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634034, Томская область, г. Томск, Вершинина улица, д. 47, 407 ауд.

Описание имеющегося оборудования:

- Доска магнитно-маркерная;
- Коммутатор D-Link Switch 24 port;
- Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. (12 шт.);
- Вольтметр В3-38 (7 шт.);
- Генератор сигналов специальной формы АКИП ГСС-120 (2 шт.);
- Кронштейн PTS-4002;
- Осциллограф EZ Digital DS-1150C (3 шт.);
- Осциллограф С1-72 (4 шт.);
- Телевизор плазменный Samsung;
- Цифровой генератор сигналов РСС-80 (4 шт.);
- Цифровой осциллограф GDS-810C (3 шт.);
- Автоматизированное лабораторное место по схемотехнике и радиоавтоматике (7 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Adobe Acrobat Reader
- Google Chrome
- Mozilla Firefox

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Учебная лаборатория "Компьютерной радиоэлектроники"

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634034, Томская область, г. Томск, Вершинина улица, д. 47, 412 ауд.

Описание имеющегося оборудования:

- Доска магнитно-маркерная;
- Компьютер Core 2 (11 шт.);
- Телевизор Samsung;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Google Chrome
- Microsoft Windows 8 и ниже

– Mozilla Firefox

13.1.4. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

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

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **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 комфортного просмотра.

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Содержание и структура законодательства в области информационной безопасности включает:

1) Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации - Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы;

2) Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента

Российской Федерации;

3) Подзаконные акты Правительства Российской Федерации – Федеральные 2законы - Кодексы;

4) нет верного ответа.

2. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации состоит из:

1) Федерального закона «Об информации, информационных технологиях и о защите информации» и других федеральных законов, регулирующих отношения в области использования информации;

2) Федерального закона «О персональных данных» и других федеральных законов, регулирующих отношения в области использования информации;

3) Федерального закона «О коммерческой тайне» и других федеральных законов, регулирующих отношения в области использования информации;

4) Федерального закона «О государственной тайне» и других федеральных законов, регулирующих отношения в области использования информации.

3. Предметом правового регулирования в области информации, информационных технологий и защиты информации являются:

1) отношения, возникающие только при осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) отношения, возникающие только при применении информационных технологий;

3) отношения, возникающие только при обеспечении защиты информации;

4) отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации.

4. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации;

4) верны все варианты.

5. Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:

1) отнесенные к государственной тайне;

2) отнесенные к служебной тайне (информации для служебного пользования), персональные данные (и другие виды тайн);

3) отнесенные к информации о прогнозах погоды;

4) все верны ответы.

6. Как называется закон, регулирующий деятельность государственной тайны на территории РФ?

1) «О коммерческой тайне»;

2) «О государственной тайне»;

3) «О служебной тайне»;

4) «О врачебной тайне».

7. Государственная тайна — это:

1) защищаемые государственные сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации;

2) защищаемые государственные сведения только в области военной и внешнеполитической деятельности, распространение которой может нанести ущерб безопасности Российской Федерации;

3) защищаемые государственные сведения только в области экономической и разведывательной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации.

4) защищаемые государственные сведения только в области внешнеполитической деятельности, распространение которой может нанести ущерб безопасности Российской Федерации;

8. Срок засекречивания сведений, составляющих государственную тайну, не должен превышать:

1) 30 лет;
2) 40 лет;
3) 50 лет;
4) 60 лет.

9. Субъект персональных данных обладает правами:

1) на доступ к своим персональным данным;

2) возражение против принятия решений исключительно на основании автоматизированной обработки персоналом данных, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы;

3) обжалование действий или бездействий;

4) верны все варианты.

10. В целях охраны конфиденциальности информации работодатель обязан:

1) ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны;

4) верны все варианты.

11. К методам обеспечения информационной безопасности не относятся:

1) корпоративные;
2) административные;
3) правовые;
4) технические.

12. Что относится к каналам, не требующим изменение элементов ИС?

1) намеренное копирование файлов и носителей информации;
2) незаконное подключение специальной регистрирующей аппаратуры;
3) злоумышленное изменение программ;
4) злоумышленный вывод из строя средств защиты информации.

13. На какой срок выдается сертификат соответствия средства защиты информации?

1) до 4 лет;
2) до 3 лет;
3) до 5 лет;
4) до 6 лет.

14. Участникам конфиденциального совещания, независимо от зажимаемой должности и

статуса на совещании, не разрешается:

а) вносить в помещение, в котором проводится совещание, фото-, кино- и видеоаппаратуру, компьютеры, магнитофоны, плейеры, диктофоны, радиоприемники, радиотелефоны и другую аппаратуру, пользоваться ею;

б) делать выписки из документов, используемых при решении вопросов на совещании и имеющих гриф ограничения доступа;

в) обсуждать вопросы, вынесенные на совещание, в местах общего пользования;

г) верны все варианты.

15. Информацию по степени доступа разделяют на:

1) открытую и ограниченного доступа;

2) открытую;

3) закрытую;

4) тайную и ограниченную.

16. На документах, предоставляемых указанным органам и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф:

1) «Коммерческая тайна»;

2) «Служебная тайна»;

3) «Деловая тайна»;

4) «Конфиденциально».

17. Сколько уровней защищенности персональных данных указано в Постановлении Правительства № 1119 от 01.11.2012:

1) 4;

2) 5;

3) 3;

4) 8.

18. Срок действия на полезную модель составляет:

1) 5 лет;

2) 10 лет;

3) 15 лет;

4) 20 лет.

19. Срок действия патента на изобретение составляет:

1) 5 лет;

2) 10 лет;

3) 15 лет;

4) 20 лет.

20. Какой документ занимает главное место в системе законодательства в области авторского права РФ?

а) Конституция РФ;

б) Уголовный Кодекс РФ;

в) Гражданский Кодекс;

г) Трудовой Кодекс.

14.1.2. 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 судо-

производства, 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.

14.1.3. 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.

14.1.4. Вопросы дифференцированного зачета

1. Информация как объект правового регулирования.

2.Государственная система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам.

3. Государственная тайна. Порядок допуска должностных лиц и граждан Российской Федерации к государственной тайне.

4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа.

5.Оценка соответствия объектов информатизации требованиям безопасности информации.

6.Классификация автоматизированных систем и требования по защите информации.

7.Специальные защитные знаки.

8.Лицензирования и сертификации в области технической защите конфиденциальной информации.

9.Система сертификации средств защиты информации о требованиям безопасности

информации.

10.Ключевые системы информационной инфраструктуры.

11.Правовой режим обеспечения безопасности персональных данных.

12.Особенности обработки персональных данных осуществляемой без использования средств автоматизации

13.Особенности обеспечения безопасности персональных данных операторами, являющимися государственными либо муниципальными органами.

14.Особенности обработки биометрических персональных данных.

15.Правовой режим обеспечения безопасности государственных и муниципальных систем.

16.Режим защиты коммерческой тайны.

14.1.5. 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.

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (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 материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов 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.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся 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 лиц с ограниченными возможностями здоровья и 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 лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.