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
_____ П. Е. Троян
«___» _____ 20__ г.

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 2015 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	Всего	Единицы
1	Лекции	24	24	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	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 2018

Согласована на портале № 40531

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 кафедра Радиоэлектроники и систем связи (РСС) _____ Д. В. Дубинин

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

Старший преподаватель кафедры радиоэлектроники и систем связи (РСС) _____ Ю. В. Зеленецкая

Согласована на портале № 40531

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.3) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информатика.

Последующими дисциплинами являются: Математические методы описания сигналов, Основы информационной безопасности сетей и систем, Техническая защита информации, Технические средства защиты информации в системах 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 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 № 40531

Практические занятия	18	18
Лабораторные работы	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, ч	108	108
Зачетные Единицы	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	Лек., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
4 семестр						
1 Введение.	2	0	0	1	3	ПК-16, 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-16, 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
9 Зачёт.	0	0	0	7	7	ПК-16, ПК-8
Итого за семестр	24	18	18	48	108	
Итого	24	18	18	48	108	

Согласована на портале № 40531

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.	2	ПК-16, 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, ПК-8
	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 области защиты информации. Правовые основы защиты информации с использованием технических средств. Система правовой ответственности за разглашение защищаемой информации и невыполнение правил ее защиты.	3	ПК-16, ПК-8
	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 интеллектуальной собственности. Основы международного законодательства в области защиты информации. Парижская конвенция по охране промышленной собственности. Договор о патентной	3	ПК-16, ПК-8

Согласована на портале № 40531

	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, ПК-8
	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-16, 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-16, 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.	4	ПК-16, 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 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									

Согласована на портале № 40531

1 Информатика						+			
Последующие дисциплины									
1 Математические методы описания сигналов								+	
2 Основы информационной безопасности сетей и систем					+				
3 Техническая защита информации		+	+		+	+	+	+	
4 Технические средства защиты информации в системах 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, Отчет по лабораторной работе, Опрос на занятиях, Зачет, Тест, Отчет по практическому занятию
ПК-16	+		+	+	Конспект самоподготовки, Отчет по лабораторной работе, Опрос на занятиях, Зачет, Тест

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.	3	ПК-8
	Итого	3	

Согласована на портале № 40531

3 Система защиты государственной тайны и конфиденциальной информации.	Разработка проектов документального оформления основных видов конфиденциальной информации.	4	ПК-8
	Итого	4	
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 (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.	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	Служба безопасности объекта.	2	ПК-8
	Итого	2	

Согласована на портале № 40531

информационной безопасности.			
6 Средства и методы физической защиты объектов.	Средства и методы физической защиты объектов. Организация пропускного и внутриобъектового режимов.	2	ПК-8
	Итого	2	
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	Трудоемкость, ч	Формируемые компетенции	Формы контроля
4 семестр				
1 Введение.	Проработка лекционного материала	1	ПК-16, ПК-8	Зачет, Конспект самоподготовки, Опрос на занятиях, Тест
	Итого	1		
2 Законодательство Российской Федерации в области информационной безопасности. Виды защищаемой информации.	Подготовка к практическим занятиям, семинарам	2	ПК-8, ПК-16	Зачет, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Отчет по практическому занятию, 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	4	ПК-8, ПК-16	Зачет, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
4 Основы защиты интеллектуальной собственности и основ международного законодательства в	Подготовка к практическим занятиям, семинарам	2	ПК-8, ПК-16	Зачет, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Проработка лекционного материала	1		

Согласована на портале № 40531

области защиты информации.	Итого	3		
5 Общие вопросы организационного обеспечения информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ПК-8, ПК-16	Зачет, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Проработка лекционного материала	1		
	Итого	3		
6 Средства и методы физической защиты объектов.	Подготовка к практическим занятиям, семинарам	2	ПК-8, ПК-16	Зачет, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Отчет по практическому занятию, 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-16, ПК-8	Зачет, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	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, ПК-16	Зачет, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	7		
9 Зачёт.	Проработка лекционного материала	7	ПК-16, ПК-8	Зачет, Тест
	Итого	7		
Итого за семестр		48		
Итого		48		

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				

Согласована на портале № 40531

Зачет			26	26
Конспект самоподготовки	4	4	4	12
Опрос на занятиях	4	4	6	14
Отчет по лабораторной работе	3	3	3	9
Отчет по практическому занятию	3	3	3	9
Тест	10	10	10	30
Итого максимум за период	24	24	52	100
Нарастающим итогом	24	48	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 / А. Н. Сычев - 2014. 240 с. - Режим доступа: https://edu.tusur.ru/publications/4967 (дата обращения: 24.07.2018).

2. Государственная и муниципальная служба РФ [Электронный ресурс]: Учебное пособие / Н. А. Грик - 2016. 97 с. - Режим доступа: https://edu.tusur.ru/publications/6121 (дата обращения: 24.07.2018).

Согласована на портале № 40531

12.2. Дополнительная литература

1. Документирование управленческой деятельности [Электронный ресурс]: Учебное пособие / Ж. Н. Аксенова - 2009. 194 с. - Режим доступа: https://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 / Л. А. Белицкая - 2011. 22 с. - Режим доступа: https://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 / Э. В. Семенов - 2012. 13 с. - Режим доступа: https://edu.tusur.ru/publications/2506 (дата обращения: 24.07.2018).
3. Защита и обработка конфиденциальных документов [Электронный ресурс]: Методические указания для практических занятий / Л. А. Белицкая - 2011. 56 с. - Режим доступа: https://edu.tusur.ru/publications/3031 (дата обращения: 24.07.2018).
4. Моделирование и анализ бизнес-процессов. Часть I [Электронный ресурс]: Методические указания для выполнения лабораторных работ по дисциплине для студентов направления "Программная инженерия" / М. П. Силич - 2014. 72 с. - Режим доступа: https://edu.tusur.ru/publications/6457 (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. При изучении дисциплины рекомендуется использовать базы данных и информационно-справочные системы, к которым у ТУСУРа есть доступ https://lib.tusur.ru/ru/resursy/bazydannyh

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

Согласована на портале № 40531

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
- Far Manager
- Google Chrome
- LibreOffice
- Microsoft Windows
- Mozilla Firefox
- PDFCreator
- WinDjView

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

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
- Far Manager

Согласована на портале № 40531

- Google Chrome
- LibreOffice
- Microsoft Windows
- Mozilla Firefox
- PDFCreator
- WinDjView

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. Законодательство Российской Федерации об информации, информационных технологиях

Согласована на портале № 40531

и о защите информации состоит из

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

2) Федерального закона «Об информации, информационных технологиях и о защите информации» 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.

2. К информации ограниченного доступа относятся

1) государственная тайна;

2) конфиденциальная информация;

3) персональные данные;

4) все ответы верны.

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

1) 45 лет

2) 50 лет

3) 30 лет

4) 35 лет

4. Персональные данные - это

1) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

2) конкретная информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

3) любая информация, относящаяся к определенному или определяемому на основании такой информации юридическому лицу (субъекту персональных данных).

4) точная информация, относящаяся к определенному или определяемому на основании такой информации юридическому лицу (субъекту персональных данных).

5. Информацию по степени доступа разделяют на

1) открытую;

2) закрытую;

3) тайную и ограниченную.

4) открытую и ограниченного доступа;

6. Под аттестацией объектов информатизации понимается:

1) комплекс организационно-технических мероприятий по проверке (аттестационным испытаниям) защищаемого объекта информатизации в реальных условиях эксплуатации;

2) анализ защищенности внешнего периметра корпоративной сети;

3) анализ защищенности внутренней ИТ-инфраструктуры;

4) аудит безопасности критичных бизнес приложений.

7. Какой орган является уполномоченным в сфере защиты прав субъектов персональных данных

1) Роскомнадзор

2) ФСБ Росси

3) ФСТЭК России

4) Все ответы правильные

8. Использование сертифицированных средств защиты информации является, не является обязательным для…

1) Коммерческой тайны

2) Налоговой тайны

3) Государственной тайны

4) Персональных данных

9. Какой официальный документ занимает главное место в системе законодательства в обла-

Согласована на портале № 40531

сти авторского права РФ

1) Конституция РФ

2) Гражданский кодекс

3) Уголовный кодекс

4) Доктрина информационной безопасности

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. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации

1) угроза

2) уязвимость

3) Инцидент ИБ

4) атака

12. По типу актуальных угроз ИСПДн подразделяются на

1) 3 типа

2) 2 типа

3) 4 типа

4) Внешние и внутренние

13. Требованиями к защите ПДн при их обработке в информационных системах (Утв. Постановлением Правительства № 1119 от 01.11.2012) установлены

1) уровни защищенности ПДн

2) Категории угроз безопасности

3) Критерии безопасности ПДн

4) Классы защищенности ПДн

14. Какой гриф ставится на носителях содержащих персональные данные

1) Гриф не ставится

2) Персональные данные

3) Конфиденциально

4) Для служебного пользования

15. К методам обеспечения информационной безопасности не относятся:

1) корпоративные

2) административные

3) технические

4) организационные

16. Не подлежат засекречиванию сведения о

1) чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях

2) сведения о военных разработках

3) сведения об антитеррористических мероприятиях

4) сведения о технических разработках

17. Для проведения работ и/или оказания услуг в области установки и настройки СКЗИ, требуется лицензия

1) ФСБ России

2) Минкомсвязи РФ

3) ФСТЭК России

4) Все варианты верные

Согласована на портале № 40531

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

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

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

3) отношения, возникающие только при обеспечении защиты информации

4) удовлетворенности руководителя проекта

19. Срок действия патента на изобретение составляет

1) 20 лет

2) 10 лет

3) 25 лет

4) 5 лет

20. Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных определяются приказом ФСТЭК №

1) 21

2) 17

3) 31

4) 152 ФЗ

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 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 интеллектуальной 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.

Согласована на портале № 40531

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. 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.

14.1.4. 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.

14.1.5. Вопросы для подготовки к практическим занятиям, семинарам

Общие вопросы. Право на информацию и его ограничения. Виды защищаемой информации.

Защита коммерческой тайны.

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

Организационно-правовая защита служебной тайны.

Служба безопасности объекта.

Средства и методы физической защиты объектов. Организация пропускного и внутриобъектового режимов.

Анализ и оценка угроз информационной безопасности объекта.

14.1.6. 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

Согласована на портале № 40531

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.

Согласована на портале № 40531