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

Организационное и правовое обеспечение информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Безопасность телекоммуникационных систем информационного взаимодействия**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РСС, Кафедра радиоэлектроники и систем связи**
Курс: **4**
Семестр: **7, 8**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	8 семестр	Всего	Единицы
1	Лекции	16	16	32	часов
2	Практические занятия	28	30	58	часов
3	Всего аудиторных занятий	44	46	90	часов
4	Самостоятельная работа	46	8	54	часов
5	Всего (без экзамена)	90	54	144	часов
6	Подготовка и сдача экзамена	0	36	36	часов
7	Общая трудоемкость	90	90	180	часов
		2.5	2.5	5.0	З.Е.

Зачет: 7 семестр
Экзамен: 8 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) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16.11.2016 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 «Организационное и правовое обеспечение информационной безопасности» (Б1.Б.17) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Защита и обработка конфиденциальных документов, Организационное и правовое обеспечение информационной безопасности.

Последующими дисциплинами являются: Организация и управление службой защиты информации на предприятии, Организационное и правовое обеспечение информационной безопасности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;
- ПК-1 способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем;
- ПК-10 способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений;

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 5.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		7 семестр	8 семестр
Аудиторные занятия (всего)	90	44	46
Лекции	32	16	16
Практические занятия	58	28	30
Самостоятельная работа (всего)	54	46	8
Проработка лекционного материала	32	28	4
Подготовка к практическим занятиям, семинарам	22	18	4
Всего (без экзамена)	144	90	54
Подготовка и сдача экзамена	36	0	36
Общая трудоемкость, ч	180	90	90
Зачетные Единицы	5.0	2.5	2.5

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	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр					
1 1. Введение.	2	0	2	4	ОК-5
2 2 Законодательство Российской Федерации в области информационной безопасности.	2	6	13	21	ПК-1, ПК-10
3 3. Виды защищаемой информации.	2	6	16	24	ПК-1, ПК-10
4 4. Система защиты государственной тайны и конфиденциальной информации.	0	12	4	16	ОК-5, ПК-1
5 5. Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	10	4	11	25	ОК-5, ПК-1, ПК-10
Итого за семестр	16	28	46	90	
8 семестр					
6 1. Общие вопросы организационного обеспечения информационной безопасности.	4	6	2	12	ОК-5, ПК-10
7 2. Средства и методы физической защиты	4	12	2	18	ОК-5, ПК-1,

объектов.					ПК-10
8 3.Организация пропускного и внутри-объектового режимов объектов.	2	6	2	10	ПК-1, ПК-10
9 4. Методика анализа и оценки угроз информационной безопасности объекта.	6	6	2	14	ОК-5, ПК-1, ПК-10
Итого за семестр	16	30	8	54	
Итого	32	58	54	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
7 семестр			
1 1. Введение.	Цели, структура и задачи курса. Понятие организационного и правового обеспечения информационной безопасности. Взаимосвязь курса с другими дисциплинами. Специфика курса.	2	ОК-5
	Итого	2	
2 2 Законодательство Российской Федерации в области информационной безопасности.	Понятие права. Отрасли права,обеспечивающие законность в областизащиты информации. Основныеинформационные права и свободы и ихограничения. Признакиохраноспособности права наинформацию с ограниченнымдоступом.	2	ПК-10
	Итого	2	
3 3. Виды защищаемой информации.	Виды защищаемойинформации: государственная тайна,служебная тайна, профессиональнаятайна, коммерческая тайна, тайнаследствия и судопроизводства,персональные данные, сведения осущности изобретения, полезноймодели или промышленного образцадо официальной публикацииинформации о них.	2	ПК-10
	Итого	2	
5 5. Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	Правовой режим защитыгосударственной тайны, закон «Огосударственной тайне». Организацияи обеспечение режима секретности.Организационно-правовая защитаслужебной тайны. Закон «Окоммерческой тайне». Закон «Оперсональных данных».Лицензирование и сертификация в3 ПК-16,ПК-863746области защиты информации.Правовые основы защиты информациис использованием техническихсредств. Система правовойответственности за разглашениезащищаемой информации иневыполнение правил ее защиты.	8	ОК-5, ПК-1, ПК-10
	Понятие интеллектуальнойсобственности. Гра-	2	

	жданский кодекс –источник норм в области защитыинтеллектуальной собственности:авторское право и смежные права,патентное право, законодательство осредствах индивидуализацииучастников гражданского оборота.Система правовой ответственности занарушения законодательства обинтеллек-туальной собственности.Основы международногозаконодательства в области защитыинформации. Парижская конвенция поохране промышленной собственности.Договор о патентной кооперации.Евразийская патентная конвенция.		
	Итого	10	
Итого за семестр		16	
8 семестр			
6 1. Общие вопросы организационного обеспечения информационной безопасности.	Принципы обеспеченияинформационной безопасности.Взаимосвязь службы безопасностипредприятия с государственнымиорганами обеспечения безопасности.Федеральная служба безопасности.-Служба специальной связи. Службабезопасности объекта. Структураслужбы безопасности объекта. Задачи,решаемые службой безопасностиобъекта.	4	ОК-5, ПК-10
	Итого	4	
7 2. Средства и методы физической защиты объектов.	Демонстративная и скрытная охрана.Охрана путем выставления постов и спомощью технических средств.Многорубежная защита. Режимохраны. Нештатные ситуации,требующие усиления режима охраны.Принцип экономичности припостроении комплексной системызащиты.	4	ПК-1
	Итого	4	
8 3.Организация пропускного и внутриобъектового режимов объектов.	Понятия пропускного ивнутриобъектового режимов.Пропускные документы.Удостоверения, постоянные,временные, разовые и материальныепропуска. Компьютерные системыконтроля доступа. Защита информациив экстремальных ситуациях.Информационная безопасностьобъекта при осуществлениимеждународного сотрудничества.	2	ПК-1, ПК-10
	Итого	2	
9 4. Методика анализа и оценки угроз информационной безопасности объекта.	Классификация угрозинформационной безопасностиобъекта. Внешние и внутренниеугрозы. Угрозы конфиденциальности,целостности, доступности данных.Типичные каналы утечки информации.Анализ и оценка рисков. Анализрисков без их числовых характеристик.Анализ рисков, включающийопределение ценности ресурсов,оценку угроз и оценку эффективностипринятых мер. Определение ценностиресурсов: физических,информационных. Оценка вероятностиреализации угроз. Оценка ущерба.	6	ОК-5, ПК-1, ПК-10
	Итого	6	

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
Предшествующие дисциплины									
1 Защита и обработка конфиденциальных документов						+			
2 Организационное и правовое обеспечение информационной безопасности	+	+	+	+	+	+	+	+	+
Последующие дисциплины									
1 Организация и управление службой защиты информации на предприятии								+	
2 Организационное и правовое обеспечение информационной безопасности	+	+	+	+	+	+	+	+	+

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.	Сам. раб.	
ОК-5	+	+	+	Контрольная работа, Домашнее задание, Выполнение контрольной работы, Собеседование, Опрос на занятиях, Консультирование, Расчетная работа, Тест
ПК-1	+	+	+	Контрольная работа, Домашнее задание, Выполнение контрольной работы, Собеседование, Опрос на занятиях, Консультирование, Расчетная работа, Тест

ПК-10	+	+	+	Контрольная работа, Домашнее задание, Выполнение контрольной работы, Конспект самоподготовки, Собеседование, Опрос на занятиях, Консультирование, Расчетная работа, Выступление (доклад) на занятии, Тест, Реферат, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

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
7 семестр			
2 2 Законодательство Российской Федерации в области информационной безопасности.	Разработка проектов документальногооформления основных видовзащищаемой информации.	6	ПК-1, ПК-10
	Итого	6	
3 3. Виды защищаемой информации.	Общие вопросы. Право наинформацию и его ограничения. Видызащищаемой информации	6	ПК-1, ПК-10
	Итого	6	
4 4. Система защиты государственной тайны и конфиденциальной информации.	Разработка проектов документальногооформления основных видовконфиденциальной информации.	12	ОК-5, ПК-1
	Итого	12	
5 5. Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	Организационно-правовая защитаслужебной тайны.	4	ПК-1
	Итого	4	
Итого за семестр		28	
8 семестр			
6 1. Общие вопросы организационного обеспечения информационной безопасности.	Служба безопасности объекта.	6	ПК-10
	Итого	6	

7 2. Средства и методы физической защиты объектов.	Средства и методы физической защитыобъектов. Организация пропускного ивнутриобъектового режимов	12	ОК-5, ПК-10
	Итого	12	
8 3.Организация пропускного и внутриобъектового режимов объектов.	Практические правила обеспечениязащиты объектов.6	6	ПК-1
	Итого	6	
9 4. Методика анализа и оценки угроз информационной безопасности объекта.	Практика анализа и оценки угрозинформационной безопасностиобъекта защиты.	6	ПК-10
	Итого	6	
Итого за семестр		30	
Итого		58	

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
7 семестр				
1 1. Введение.	Проработка лекционного материала	2	ОК-5	Собеседование, Тест
	Итого	2		
2 2 Законодательство Российской Федерации в области информационной безопасности.	Подготовка к практическим занятиям, семинарам	4	ПК-1, ПК-10	Домашнее задание, Консультирование, Опрос на занятиях, Расчетная работа, Тест
	Проработка лекционного материала	9		
	Итого	13		
3 3. Виды защищаемой информации.	Подготовка к практическим занятиям, семинарам	6	ПК-1, ПК-10	Выполнение контрольной работы, Домашнее задание, Конспект самоподготовки, Консультирование, Контрольная работа, Опрос на занятиях, Отчет по практическому занятию, Расчетная работа, Реферат, Собеседование, Тест
	Проработка лекционного материала	10		
	Итого	16		
4 4. Система защиты государственной тайны и конфиденциальной информации.	Подготовка к практическим занятиям, семинарам	4	ОК-5, ПК-1	Выполнение контрольной работы, Расчетная работа, Тест
	Итого	4		

5 5. Основы защиты интеллектуальной собственности и основ международного законодательства в области защиты информации.	Подготовка к практическим занятиям, семинарам	4	ПК-1, ОК-5, ПК-10	Выполнение контрольной работы, Домашнее задание, Конспект самоподготовки, Консультирование, Тест
	Проработка лекционного материала	6		
	Проработка лекционного материала	1		
	Итого	11		
Итого за семестр		46		
8 семестр				
6 1. Общие вопросы организационного обеспечения информационной безопасности.	Подготовка к практическим занятиям, семинарам	1	ПК-10, ОК-5	Выступление (доклад) на занятии, Опрос на занятиях, Собеседование, Тест
	Проработка лекционного материала	1		
	Итого	2		
7 2. Средства и методы физической защиты объектов.	Подготовка к практическим занятиям, семинарам	1	ОК-5, ПК-10, ПК-1	Выполнение контрольной работы, Домашнее задание, Консультирование, Контрольная работа, Собеседование, Тест
	Проработка лекционного материала	1		
	Итого	2		
8 3.Организация пропускного и внутриобъектового режимов объектов.	Подготовка к практическим занятиям, семинарам	1	ПК-1, ПК-10	Опрос на занятиях, Собеседование, Тест
	Проработка лекционного материала	1		
	Итого	2		
9 4. Методика анализа и оценки угроз информационной безопасности объекта.	Подготовка к практическим занятиям, семинарам	1	ПК-10, ОК-5, ПК-1	Домашнее задание, Контрольная работа, Тест
	Проработка лекционного материала	1		
	Итого	2		
Итого за семестр		8		
	Подготовка и сдача экзамена	36		Экзамен
Итого		90		

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	Максимальный	Максимальный	Максимальный	Всего за

деятельности	балл на 1-ую КТ с начала семестра	балл за период между 1КТ и 2КТ	балл за период между 2КТ и на конец семестра	семестр
7 семестр				
Выполнение контрольной работы	5	5	5	15
Домашнее задание	5	5	5	15
Конспект самоподготовки	3	3	3	9
Консультирование	1	1	1	3
Опрос на занятиях	3	3	3	9
Отчет по практическому занятию		3	4	7
Расчетная работа	3	3	3	9
Реферат	2	2	2	6
Собеседование	2	2	2	6
Тест	7	7	7	21
Итого максимум за период	31	34	35	100
Нарастающим итогом	31	65	100	100
8 семестр				
Выполнение контрольной работы	5	5	6	16
Выступление (доклад) на занятии	4	4	5	13
Домашнее задание	5	6	6	17
Консультирование			1	1
Контрольная работа	2	2	3	7
Опрос на занятиях	1	1	2	4
Собеседование	2	2	2	6
Тест	2	2	2	6
Итого максимум за период	21	22	27	70
Экзамен				30
Нарастающим итогом	21	43	70	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 для бакалавров / Н. А. Грик - 2016. 97 с. - Режим доступа: https://edu.tusur.ru/publications/6131 (дата обращения: 24.07.2018).

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).

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
- Far Manager
- Google Chrome
- Microsoft Windows

13.1.3. 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. Экзаменационные вопросы

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.
17. Перечислите способы защиты авторских и смежных прав.
18.Базовые источники правового обеспечения информационной безопасности.
19. Преступления в сфере компьютерной информации.
20. Особенности внутриобъектового режима.
21. Особенности лицензирование в информационной безопасности.
22.Особенности сертификации средств защиты информации.

14.1.3. Темы докладов

1. Правовое регулирование в РФ.
2. Государственная система защиты информации в РФ.
3. Виды защищаемой информации.
4. Государственная тайна.
5. Лицензирование и сертификация.
6. Патентное и авторское право
7. Менеджмент в информационной безопасности

14.1.4. Темы домашних заданий

1. Лицензирования и сертификации в области технической защите конфиденциальной информации.
2. Система сертификации средств защиты информации о требованиям безопасности информации.
3. Классификация угроз информационной безопасности объекта. Внешние и внутренние угрозы. Угрозы конфиденциальности, целостности, доступности данных. Типичные каналы утечки информации. Анализ и оценка рисков.
4. Основные законодательные акты, регулирующие обеспечение безопасности персональных данных.
5. Организация пропускного и внутриобъектового режимов объектов.
6. Средства и методы физической защиты объектов

14.1.5. Вопросы на собеседование

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.

14.1.6. Темы опросов на занятиях

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.
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.

14.1.7. Темы рефератов

1.Негативное воздействие на компьютерную информацию.

2.Современные вредоносные программы. Способы и средства преднамеренного негативного воздействия на компьютерную информацию.

3. Меры, способы и средства защиты компьютерной информации и информации в сфере высоких технологий.

4. Основы защиты сведений, составляющих государственную тайну; методы защиты информации.

5. Резервирование и архивирование компьютерной информации. Защита архивов от несанкционированного доступа.

6. Специальные средства и утилиты в сфере компьютерных и высоких технологий.

7. Восстановление преднамеренно удаленной или скрытой информации.

8. Современные автоматизированные информационные системы юридического характера. Автоматизированные банки данных.

9. Информационные правоотношения. Понятие и специфика компьютерных преступлений.

10.Способы совершения преступлений в области компьютерных и высоких технологий.

11.Информационная безопасность.Методы защиты информации.Компьютерные преступления.

12. Электронный документооборот и электронная цифровая подпись.

13. Персональные данные и Интернет.

14.1.8. Темы контрольных работ

1. Информационное оружие: понятие и направления применения.

2. Электронная подпись: понятие, виды, цели использования.

3. Понятие информационной безопасности. Разграничение понятий «безопасность информации», «защита информации» и «компьютерная безопасность».

4. Основные нормативные правовые акты, регламентирующие обеспечение информационной безопасности.

5. Система органов, ответственных за обеспечение информационной безопасности в Российской Федерации: общая характеристика.

6. Угрозы информационной безопасности, их классификация

7. Правовая ответственность за правонарушения в сфере информационной безопасности.

14.1.9. 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.

14.1.10. Вопросы для подготовки к практическим занятиям, семинарам

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.

14.1.11. Темы расчетных работ

1. Разработка частной модели угроз безопасности информационной системы персональных данных

2.Разработка модели нарушителя объекта информатизации

3. Разработка частного технического задания на проектирование системы защиты информации

14.1.12. 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.

14.2. 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.