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

Информационная безопасность телекоммуникационных систем

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: **5**
Семестр: **10**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Практические занятия	38	38	часов
3	Лабораторные работы	34	34	часов
4	Всего аудиторных занятий	108	108	часов
5	Самостоятельная работа	72	72	часов
6	Всего (без экзамена)	180	180	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	216	216	часов
		6.0	6.0	З.Е.

Экзамен: 10 семестр

Томск 2018

Согласована на портале № 38705

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. П. Кшнянкин
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:

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

Согласована на портале № 38705

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является формирование у студентов устойчивых основ знаний организации информационной безопасности телекоммуникационных систем и методов ее управления, приобретения при этом необходимых умений и навыков.

1.2. Задачи дисциплины

– Основными задачами изучения дисциплины являются:

– • изучение сущности и задач системы защиты информации (СЗИ) телекоммуникационных систем (ТКС);

– • изучение принципов организации и этапов разработки СЗИ ТКС, факторов, влияющих на организацию СЗИ ТКС;

– • определение и нормативное закрепление состава защищаемой информации; определение объектов защиты;

– • анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию;

– • определение потенциальных каналов и методов несанкционированного доступа к информации, определение возможностей несанкционированного доступа к защищаемой информации;

– • определение компонентов и условий функционирования СЗИ ТКС, разработка модели, технологического и организационного построения СЗИ ТКС;

– • кадровое, материально-техническое и нормативно-методическое обеспечение функционирования СЗИ ТКС;

– • назначение, структура и содержание управления СЗИ ТКС, изучение принципов и методы планирования, сущности и содержание контроля функционирования СЗИ ТКС;

– • изучение особенностей управления СЗИ ТКС в условиях чрезвычайных ситуаций;

– • изучение состава методов и моделей оценки эффективности СЗИ ТКС.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность телекоммуникационных систем» (Б1.Б.36) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Защита и обработка конфиденциальных документов, Информационные технологии, Криптографические методы защиты информации, Организационное и правовое обеспечение информационной безопасности, Организация и управление службой защиты информации на предприятии, Основы информационной безопасности, Техническая защита информации.

Последующими дисциплинами являются: Преддипломная практика.

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-6 способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду;

В результате изучения дисциплины обучающийся должен:

– **знать** Основы организации и управления системой защиты информации телекоммуникационных систем.

– **уметь** На концептуальном и практическом уровне разрабатывать и внедрять системы защиты информации телекоммуникационных систем.

– **владеть** Навыками внедрения систем защиты информации телекоммуникационных си-

Согласована на портале № 38705

стем.

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
		10 семестр
Аудиторные занятия (всего)	108	108
Лекции	36	36
Практические занятия	38	38
Лабораторные работы	34	34
Самостоятельная работа (всего)	72	72
Оформление отчетов по лабораторным работам	34	34
Проработка лекционного материала	38	38
Всего (без экзамена)	180	180
Подготовка и сдача экзамена	36	36
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
10 семестр						
1 Введение.	1	2	0	2	5	ОК-5
2 Содержание и этапы проведения работ по организации системы защиты информации телекоммуникационных систем (СЗИ ТКС).	5	4	0	4	13	ПК-6
3 Определение компонентов СЗИ ТКС.	9	4	0	4	17	ПК-6
4 Технология определения и классификации состава и защищенности информации.	7	8	0	6	21	ПК-6
5 Построение системы защиты информации телекоммуникационных систем.	4	14	18	4	40	ПК-6
6 Управление системой защиты информации телекоммуникационных систем.	2	6	16	6	30	ПК-6
7 Служба защиты информации.	4	0	0	4	8	ПК-6
8 Особенностей управления СЗИ ТКС	2	0	0	4	6	ПК-6

Согласована на портале № 38705

в условиях чрезвычайных ситуаций.						
9 Состав методов и моделей оценки эффективности СЗИ ТКС.	2	0	0	4	6	ПК-6
10 Экзамен	0	0	0	34	34	ПК-6
Итого за семестр	36	38	34	72	180	
Итого	36	38	34	72	180	

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
10 семестр			
1 Введение.	Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер научно-технических проблем при решении задач по организации и управлению комплексной системы защиты информации на предприятии. Специфика курса.	1	ОК-5
	Итого	1	
2 Содержание и этапы проведения работ по организации системы защиты информации телекоммуникационных систем (СЗИ ТКС).	Цели системы защиты информации телекоммуникационных систем (СЗИ ТКС) и способы ее обеспечения. Системный метод при решении задач обеспечения СЗИ ТКС.Определение возможных каналов утечки информации. Определение объектов и элементов защиты.Оценка угроз технических разведок (ТР) и других источников угроз безопасности защищаемой информации. Выбор методов и средств защиты информации.	5	ПК-6
	Итого	5	
3 Определение компонентов СЗИ ТКС.	Правовая защита информации. Законодательная база РФ по защите информации (ЗИ). Сертификация и лицензирование. Правовые нормы, методы и средства защиты охраняемой информации в РФ. Система юридической ответственности за нарушение норм защиты государственной, служебной и коммерческой тайны в РФ. Правовые основы выявления и предупреждения утечки охраняемой информации.Техническая защита информации. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты и их классификация. Каналы утечки информации (оптический, акустический, радиоэлектронный). Методы защиты от несанкционированного перехвата речевой, визуальной, оптической, радиоэлектронной информации. Радиомониторинг. Криптографическая защита информации. Средства	9	ПК-6

Согласована на портале № 38705

	и методы.Физическая защита информации. Принципы, силы, средства и условия организационной защиты информации. Организация внутриобъектового и пропускного режима предприятия. Организация системы охраны предприятия (физическая охрана, пожарная и охранная сигнализация, охранное телевидение, системы ограничения доступа). Организация аналитической работы по предупреждению перехвата конфиденциальной информации. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Определение политики защиты информации на предприятии. Особенности организации комплексной защиты информации, отнесенной в установленном порядке к государственной тайне. Определение сил и средств, необходимых для защиты информации.		
	Итого	9	
4 Технология определения и классификации состава и защищенности информации.	Охраняемые сведения и объекты защиты.Особенности отнесения сведений, составляющих служебную, конфиденциальную, коммерческую и государственную тайну к различным степеням и категориям доступа.	7	ПК-6
	Итого	7	
5 Построение системы защиты информации телекоммуникационных систем.	Разработка моделей систем защиты информации телекоммуникационных систем. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования СЗИ ТКС.Архитектурное построение системы защиты информации.	4	ПК-6
	Итого	4	
6 Управление системой защиты информации телекоммуникационных систем.	Структура и содержание технологии управления системы защиты информации телекоммуникационных систем. Планирование и оперативное управление системой ЗИ, управление СЗИ ТКС в условиях чрезвычайных ситуаций.Анализ надежности функционирования системы защиты информации телекоммуникационных систем.	2	ПК-6
	Итого	2	
7 Служба защиты информации.	Организация службы защиты информации (СлЗИ) и организационное проектирование деятельности СлЗИ. Порядок создания СлЗИ, состав нормативных документов, регламентирующих деятельность служб защиты информации.	4	ПК-6
	Итого	4	
8 Особенностей управления СЗИ ТКС в условиях чрезвычайных	Определение и понятие чрезвычайной ситуации. Аспекты обеспечения условий непрерывности в информационной сфере организации. Роль совета	2	ПК-6

Согласована на портале № 38705

ситуаций.	директоров и исполнительных органов организации. Идентификация недостатков. Непрерывность сервисов в изменяющейся среде и обеспечение СЗИ ТКС. Реорганизация и ликвидация СЗИ. Определение должностного состава и численности СЗИ. Планирование и отчетность о деятельности СЗИ ТКС.Понимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер СЗИ ТКС.Восстановление после чрезвычайной ситуации функций и механизмов СЗИ ТКС. организации. Организационная основа процессов восстановления, вопросы системы менеджмента информационной безопасности (ИБ) организации и менеджмента непрерывности бизнеса. Восстановление и обеспечение функционирования процессов системы менеджмента ИБ организации.		
	Итого	2	
9 Состав методов и моделей оценки эффективности СЗИ ТКС.	Основные термины и определения, характеризующие эффективность системы защиты информации. Содержание и особенности методологии оценки эффективности СЗИ ТКС.Основные модели оценки эффективности СЗИ ТКС.	2	ПК-6
	Итого	2	
Итого за семестр		36	

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

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

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин									
	1	2	3	4	5	6	7	8	9	10
Предшествующие дисциплины										
1 Защита и обработка конфиденциальных документов		+			+	+				+
2 Информационные технологии		+	+	+	+					+
3 Криптографические методы защиты информации			+							+
4 Организационное и правовое обеспечение информационной безопасности		+				+	+			+
5 Организация и управление службой защиты информации на предприятии						+	+	+		+
6 Основы информацион-			+							+

Согласована на портале № 38705

ной безопасности										
7 Техническая защита информации		+	+	+	+				+	+
Последующие дисциплины										
1 Преддипломная практика		+	+	+	+	+	+	+	+	

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.	
ОК-5	+	+		+	Экзамен, Конспект самоподготовки, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию
ПК-6	+	+	+	+	Экзамен, Конспект самоподготовки, Отчет по лабораторной работе, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию

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
10 семестр			
5 Построение системы защиты информации телекоммуникационных систем.	Система защиты информации от несанкционированного доступа SecretNet.	6	ПК-6
	Защита информации от программных воздействий на базе антивируса Dr.Web.	6	
	Защита информации от программных воздействий на базе антивируса KAV.	6	
	Итого	18	

Согласована на портале № 38705

6 Управление системой защиты информации телекоммуникационных систем.	Система защиты информации от несанкционированного доступа Dallas Lock.	6	ПК-6
	Система защиты информации от несанкционированного доступа Страж NT.	6	
	DLP-решения по защите информации в информационных системах.	4	
	Итого	16	
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
10 семестр			
1 Введение.	Сущность и понятие системы защиты информации с позиции системного подхода.	2	ОК-5
	Итого	2	
2 Содержание и этапы проведения работ по организации системы защиты информации телекоммуникационных систем (СЗИ ТКС).	Сущность и понятие объекта защиты информации, объекта информатизации.	4	ПК-6
	Итого	4	
3 Определение компонентов СЗИ ТКС.	Определение, понятие и физический смысл технического канала утечки информации (ТКУИ). Методология защиты информации от утечки по техническим каналам.	4	ПК-6
	Итого	4	
4 Технология определения и классификации состава и защищенности информации.	Помещения, предназначенные для конфиденциальных переговоров. ТКУИ, характерные для объекта защиты. Определения и понятия. Методика защиты информации.Обработка защищаемой информации с использованием технических средств и систем. ТКУИ, характерные для объекта защиты. Определения и понятия.Методика защиты информации.	8	ПК-6
	Итого	8	
5 Построение системы защиты информации телекоммуникационных систем.	Защита информации от несанкционированного доступа (НСД). Основные определения и понятия. Особенности защиты от НСД к информации в автоматизированных системах и средствах вычислительной техники.Модель угроз и нарушителя. Понятие и основные практические подходы к разработке.Средства защиты информации по ТКУИ.	14	ПК-6

Согласована на портале № 38705

	Особенности выбора и обоснования.		
	Итого	14	
6 Управление системой защиты информации телекоммуникационных систем.	Аттестация объектов информатизации по требованиям безопасности информации. Основные понятия и особенности практической реализации. Состав примерного комплекта документов.	6	ПК-6
	Итого	6	
Итого за семестр		38	

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
10 семестр				
1 Введение.	Проработка лекционного материала	2	ОК-5	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Итого	2		
2 Содержание и этапы проведения работ по организации системы защиты информации телекоммуникационных систем (СЗИ ТКС).	Проработка лекционного материала	4	ПК-6	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Итого	4		
3 Определение компонентов СЗИ ТКС.	Проработка лекционного материала	4	ПК-6	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Итого	4		
4 Технология определения и классификации состава и защищенности информации.	Проработка лекционного материала	6	ПК-6	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Итого	6		
5 Построение системы защиты информации телекоммуникационных систем.	Проработка лекционного материала	4	ПК-6	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Итого	4		
6 Управление системой защиты информации телекоммуникационных систем.	Проработка лекционного материала	6	ПК-6	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Итого	6		
7 Служба защиты информации.	Проработка лекционного материала	4	ПК-6	Выступление (доклад) на занятии, Конспект само-

Согласована на портале № 38705

	Итого	4		подготовки, Опрос на занятиях, Тест, Экзамен
8 Особенностей управления СЗИ ТКС в условиях чрезвычайных ситуаций.	Проработка лекционного материала	4	ПК-6	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Итого	4		
9 Состав методов и моделей оценки эффективности СЗИ ТКС.	Проработка лекционного материала	4	ПК-6	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Итого	4		
10 Экзамен	Оформление отчетов по лабораторным работам	34	ПК-6	Отчет по лабораторной работе, Тест
	Итого	34		
Итого за семестр		72		
	Подготовка и сдача экзамена	36		Экзамен
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
10 семестр				
Выступление (доклад) на занятии	5	5	5	15
Конспект самоподготовки	2	2	3	7
Опрос на занятиях	2	2	4	8
Отчет по лабораторной работе	3	3	4	10
Отчет по практическому занятию	5	5	5	15
Тест	5	5	5	15
Итого максимум за период	22	22	26	70
Экзамен				30
Нарастающим итогом	22	44	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

Согласована на портале № 38705

≥ 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 информации в инфокоммуникационных системах и сетях [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2015. 284 с. - Режим доступа: https://edu.tusur.ru/publications/5262 (дата обращения: 11.07.2018).

12.2. Дополнительная литература

1. Защита информации от утечки по техническим каналам [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2015. 256 с. - Режим доступа: https://edu.tusur.ru/publications/5263 (дата обращения: 11.07.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информации в инфокоммуникационных системых и сетях [Электронный ресурс]: Учебное пособие для практических и семинарских занятий (Часть 1) / А. М. Голиков - 2015. 103 с. - Режим доступа: https://edu.tusur.ru/publications/5330 (дата обращения: 11.07.2018).
2. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: Сборник лабораторных работ / А. М. Голиков - 2012. 374 с. - Режим доступа: https://edu.tusur.ru/publications/1050 (дата обращения: 11.07.2018).
3. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / А. М. Голиков - 2017. 655 с. - Режим доступа: https://edu.tusur.ru/publications/7079 (дата обращения: 11.07.2018).

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;

Согласована на портале № 38705

– 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. Базовые законодательные и нормативно-правовые документы РФ в области защиты информации. [Электронный ресурс]. - Режим доступа: http://www.consultant.ru, (дата обращения 25.06.2018);
2. Научно-образовательный портал ТУСУРа, https://edu.tusur.ru;
3. https://lib.tusur.ru/ru/resursy/bazy-dannyh.

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
– LibreOffice
– Microsoft Windows

Согласована на портале № 38705

– Mozilla Thunderbird
– 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
– Google Chrome
– LibreOffice
– Mathworks Matlab
– Mathworks Simulink 6.5
– 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;

Согласована на портале № 38705

- 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. Как определяется системный подход и его понятие.
2. Дать понятие системы обеспечения информационной безопасности организации.
3. Система защиты информации организации, понятие и взаимосвязь с другими разделами дисциплины.
4. Защищаемая информация, определение и понятие.
5. Организация защиты информации на предприятии, существо и методика.
6. Техника защиты информации. Определение, понятие и взаимосвязь с другими разделами дисциплины.
7. Контролируемая зона. Определение, понятие, цели и задачи установления.
8. Технический канал утечки информации (ТКУИ). Понятие и физический смысл.
9. Подсистема технической защиты информации на предприятии. Определение, понятие, состав, роль и место в обеспечении защиты информации.
10. Подсистема организационно-правовой защиты информации на предприятии. Определение, понятие, структура и состав, роль и место в обеспечении защиты информации.
11. Подсистема криптографической защиты информации. Определение, понятие, состав, роль и место в обеспечении защиты информации.
12. Подсистема физической защиты информации на предприятии. Определение, понятие, структура и состав, роль и место в обеспечении защиты информации.
13. Модель угроз безопасности информации объекта информатизации на предприятии. Определение, понятие, структура и состав, роль и место в обеспечении защиты информации.
14. Модель нарушителя информационной безопасности. Определение, понятие, структура и состав, роль и место в обеспечении защиты информации.
15. Модель технической реализации подсистемы технической защиты информации объектов информатизации на предприятии. Понятие, структура и состав, роль и место в обеспечении защиты информации.

Согласована на портале № 38705

16. Автоматизированная система. Определение, понятие и взаимосвязь с другими разделами дисциплины.

17. Система защиты информации от несанкционированного доступа в автоматизированной системе. Определение, понятие и взаимосвязь с другими разделами дисциплины.

18. Сеть связи. Определение, понятие и взаимосвязь с другими разделами дисциплины.

19. Электросвязь. Определение, понятие и взаимосвязь с другими разделами дисциплины.

20. Информационная безопасность телекоммуникационных систем. Определение и понятие.

14.1.2. Экзаменационные вопросы

1. Информационная безопасность ТКС. Объект ИТКС. Определение и понятие.

2. Системный подход. Определение и понятие.

3. Модель системы обеспечения информационной безопасности организации. Определение и понятие.

4. Модель системы защиты информации организации. Определение и понятие.

5. Модель объекта защиты информации. Определение и понятие.

6. Модель защищаемой информации. Определение и понятие.

7. Модель защиты информации. Определение и понятие.

8. Модель организации защиты информации. Определение и понятие.

9. Техника защиты информации. Определение и понятие.

10. Модель контроля защиты информации. Цель и понятие.

11. Контролируемая зона. Определение и понятие.

12. Модель технического канала утечки информации (ТКУИ), виды ТКУИ. Определение, понятие, физический смысл.

13. Модель подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. Понятие.

14. Модель подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем.

Понятие.

15. Модель угроз подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем.

16. Модель угроз подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров.

17. Модель уязвимостей системы обеспечения ИБ организации. Определение и понятие.

18. Модель нарушителя ИБ организации. Определение и понятие.

19. Модель технической реализации ПТЗИ ОИ.

20. Модель нейтрализации угроз БИ на предприятии.

21. Модель подсистемы физической защиты информации объекта информатизации на предприятии.

22. Модель периметральной защиты объекта информатизации на предприятии.

23. Модель защиты информации от несанкционированного доступа (НСД). Определение и понятие.

24. Основа концепции защиты СВТ и АС от НСД к информации.

25. Классификация АС. Цели и основные понятия.

26. Аттестация объектов информатизации. Понятие.

27. Модель приобретения ПЭВМ в защищенном исполнении.

28. Доктрина ИБ РФ. Общие положения.

14.1.3. Темы докладов

1. Содержание и этапы проведения работ по организации системы защиты информации телекоммуникационных систем (СЗИ ТКС).

2.Определение компонентов СЗИ ТКС.

3. Технология определения и классификации состава и защищенности информации.

4. Построение системы защиты информации телекоммуникационных систем.

Согласована на портале № 38705

5. Управление системой защиты информации телекоммуникационных систем.
6. Служба защиты информации.

8 Особенностей управления СЗИ ТКС в условиях чрезвычайных ситуаций.

9 Состав методов и моделей оценки эффективности СЗИ ТКС.

14.1.4. Темы опросов на занятиях

Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер научно-технических проблем при решении задач по организации и управлению комплексной системы защиты информации на предприятии. Специфика курса.

Цели системы защиты информации телекоммуникационных систем (СЗИ ТКС) и способы ее обеспечения. Системный метод при решении задач обеспечения СЗИ ТКС.Определение возможных каналов утечки информации. Определение объектов и элементов защиты.Оценка угроз технических разведок (ТР) и других источников угроз безопасности защищаемой информации. Выбор методов и средств защиты информации.

Правовая защита информации. Законодательная база РФ по защите информации (ЗИ). Сертификация и лицензирование. Правовые нормы, методы и средства защиты охраняемой информации в РФ. Система юридической ответственности за нарушение норм защиты государственной, служебной и коммерческой тайны в РФ. Правовые основы выявления и предупреждения утечки охраняемой информации.Техническая защита информации. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты и их классификация. Каналы утечки информации (оптический, акустический, радиоэлектронный). Методы защиты от несанкционированного перехвата речевой, визуальной, оптической, радиоэлектронной информации. Радиомониторинг. Криптографическая защита информации. Средства и методы.Физическая защита информации. Принципы, силы, средства и условия организационной защиты информации. Организация внутриобъектового и пропускного режима предприятия. Организация системы охраны предприятия (физическая охрана, пожарная и охранная сигнализация, охранное телевидение, системы ограничения доступа). Организация аналитической работы по предупреждению перехвата конфиденциальной информации. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Определение политики защиты информации на предприятии. Особенности организации комплексной защиты информации, отнесенной в установленном порядке к государственной тайне. Определение сил и средств, необходимых для защиты информации.

Охраняемые сведения и объекты защиты.Особенности отнесения сведений, составляющих служебную, конфиденциальную, коммерческую и государственную тайну к различным степеням и категориям доступа.

Разработка моделей систем защиты информации телекоммуникационных систем. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования СЗИ ТКС.Архитектурное построение системы защиты информации.

Структура и содержание технологии управления системы защиты информации телекоммуникационных систем. Планирование и оперативное управление системой ЗИ, управление СЗИ ТКС в условиях чрезвычайных ситуаций.Анализ надежности функционирования системы защиты информации телекоммуникационных систем.

Организация службы защиты информации (СлЗИ) и организационное проектирование деятельности СлЗИ. Порядок создания СлЗИ, состав нормативных документов, регламентирующих деятельность служб защиты информации.

Определение и понятие чрезвычайной ситуации. Аспекты обеспечения условий непрерывности в информационной сфере организации. Роль совета директоров и исполнительных органов организации. Идентификация недостатков. Непрерывность сервисов в изменяющейся среде и обеспечение СЗИ ТКС. Реорганизация и ликвидация СЗИ. Определение должностного состава и численности СЗИ. Планирование и отчетность о деятельности СЗИ ТКС.Понимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер СЗИ ТКС.Восстановление после чрезвычайной ситуации функций и механизмов СЗИ ТКС. организации. Организационная основа процессов восстановления, вопросы системы менеджмента инфор-

Согласована на портале № 38705

мационной безопасности (ИБ) организации и менеджмента непрерывности бизнеса. Восстановление и обеспечение функционирования процессов системы менеджмента ИБ организации.

Основные термины и определения, характеризующие эффективность системы защиты информации. Содержание и особенности методологии оценки эффективности СЗИ ТКС.Основные модели оценки эффективности СЗИ ТКС.

14.1.5. Вопросы на самоподготовку

1. Информационная безопасность ТКС. Объект ИТКС. Определение и понятие.
2. Системный подход. Определение и понятие.
3. Модель системы обеспечения информационной безопасности организации. Определение и понятие.
4. Модель системы защиты информации организации. Определение и понятие.
5. Модель объекта защиты информации. Определение и понятие.
6. Модель защищаемой информации. Определение и понятие.
7. Модель защиты информации. Определение и понятие.
8. Модель организации защиты информации. Определение и понятие.
9. Техника защиты информации. Определение и понятие.
10. Модель контроля защиты информации. Цель и понятие.
11. Контролируемая зона. Определение и понятие.
12. Модель технического канала утечки информации (ТКУИ), виды ТКУИ. Определение, понятие, физический смысл.
13. Модель подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. Понятие.
14. Модель подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем. Понятие.
15. Модель угроз подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем.
16. Модель угроз подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров.
17. Модель уязвимостей системы обеспечения ИБ организации. Определение и понятие.
18. Модель нарушителя ИБ организации. Определение и понятие.
19. Модель технической реализации ПТЗИ ОИ.
20. Модель нейтрализации угроз БИ на предприятии.
21. Модель подсистемы физической защиты информации объекта информатизации на предприятии.
22. Модель периметральной защиты объекта информатизации на предприятии.
23. Модель защиты информации от несанкционированного доступа (НСД). Определение и понятие.
24. Основа концепции защиты СВТ и АС от НСД к информации.
25. Классификация АС. Цели и основные понятия.
26. Аттестация объектов информатизации. Понятие.
27. Модель приобретения ПЭВМ в защищенном исполнении.
28. Доктрина ИБ РФ. Общие положения.

14.1.6. Вопросы для подготовки к практическим занятиям, семинарам

Сущность и понятие системы защиты информации с позиции системного подхода.

Сущность и понятие объекта защиты информации, объекта информатизации.

Определение, понятие и физический смысл технического канала утечки информации (ТКУИ). Методология защиты информации от утечки по техническим каналам.

Помещения, предназначенные для конфиденциальных переговоров. ТКУИ, характерные для объекта защиты. Определения и понятия. Методика защиты информации.Обработка защищаемой информации с использованием технических средств и систем. ТКУИ, характерные для объекта за-

Согласована на портале № 38705

щиты. Определения и понятия.Методика защиты информации.

Защита информации от несанкционированного доступа (НСД). Основные определения и понятия. Особенности защиты от НСД к информации в автоматизированных системах и средствах вычислительной техники.Модель угроз и нарушителя. Понятие и основные практические подходы к разработке.Средства защиты информации по ТКУИ. Особенности выбора и обоснования.

Аттестация объектов информатизации по требованиям безопасности информации. Основные понятия и особенности практической реализации. Состав примерного комплекта документов.

14.1.7. Темы лабораторных работ

Система защиты информации от несанкционированного доступа SecretNet.
Система защиты информации от несанкционированного доступа Dallas Lock.
Система защиты информации от несанкционированного доступа Страж NT.
DLP-решения по защите информации в информационных системах.
Защита информации от программных воздействий на базе антивируса Dr.Web.
Защита информации от программных воздействий на базе антивируса KAV.

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.

Согласована на портале № 38705

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 № 38705