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

Принципы построения систем 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: **3**
Семестр: **5**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	26	26	часов
2	Практические занятия	36	36	часов
3	Контроль самостоятельной работы (курсовой проект / курсовая работа)	10	10	часов
4	Всего аудиторных занятий	72	72	часов
5	Самостоятельная работа	36	36	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 5 семестр

Томск 2018

Согласована на портале № 40662

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 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 № 40662

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является формирование у студентов устойчивых основ знаний о принципах построения систем информационной безопасности телекоммуникационных систем, приобретения при этом необходимых умений и навыков.

1.2. Задачи дисциплины

– Основными задачами изучения дисциплины являются:

– • изучение сущности и задач систем информационной безопасности (СИБ);

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

– • 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 СИБ, разработка модели, технологического и организационного построения СИБ;

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

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

– • изучение особенностей управления СИБ в условиях чрезвычайных ситуаций;

– • изучение состава методов и моделей оценки эффективности СИБ.

2. Место дисциплины в структуре ОПОП

Дисциплина «Принципы построения систем информационной безопасности» (Б1.В.ДВ.3.2) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы информационной безопасности.

Последующими дисциплинами являются: Защита и обработка конфиденциальных документов, Криптографические методы защиты информации, Организационное и правовое обеспечение информационной безопасности, Организация и управление службой защиты информации на предприятии, Программно-аппаратные средства обеспечения информационной безопасности, Техническая защита информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-14 способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем;

– ПК-15 способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания;

В результате изучения дисциплины обучающийся должен:

– **знать** основы организации и управления системой информационной безопасности телекоммуникационных систем на предприятии.

– **уметь** на концептуальном и практическом уровне разрабатывать и внедрять системы информационной безопасности телекоммуникационных систем на предприятии.

– **владеть** навыками внедрения систем информационной безопасности телекоммуникационных систем на предприятии.

Согласована на портале № 40662

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		5 семестр
Аудиторные занятия (всего)	72	72
Лекции	26	26
Практические занятия	36	36
Контроль самостоятельной работы (курсовой проект / курсовая работа)	10	10
Самостоятельная работа (всего)	36	36
Подготовка к практическим занятиям, семинарам	36	36
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	144	144
Зачетные Единицы	4.0	4.0

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	КП/КР, ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
5 семестр						
1 Введение	2	4	10	1	7	ПК-14, ПК-15
2 Содержание и этапы проведения работ по организации систем информационной безопасности (СИБ) телекоммуникационных систем (ТКС) на предприятии.	2	4		5	11	ПК-14, ПК-15
3 Определение компонентов СИБ.	6	4		4	14	ПК-14, ПК-15
4 Технология определения и классификации состава и защищенности информации	2	4		4	10	ПК-14, ПК-15
5 Построение СИБ телекоммуникационных систем на предприятии.	5	4		5	14	ПК-14, ПК-15
6 Управление СИБ ТКС.	2	4		4	10	ПК-14, ПК-15
7 Служба защиты информации	2	4		4	10	ПК-14, ПК-15
8 Особенности управления СИБ ТКС в условиях чрезвычайных ситуаций	3	4		5	12	ПК-14, ПК-15
9 Состав методов и моделей оценки	2	4		4	10	ПК-14, ПК-15

Согласована на портале № 40662

эффективности СИБ.						
Итого за семестр	26	36	10	36	108	
Итого	26	36	10	36	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
5 семестр			
1 Введение	Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер научно-технических проблем при решении задач по организации и управлению системой информационной безопасности телекоммуникационных систем на предприятии. Специфика курса.	2	ПК-14, ПК-15
	Итого	2	
2 Содержание и этапы проведения работ по организации систем информационной безопасности (СИБ) телекоммуникационных систем (ТКС) на предприятии.	Цели комплексной защиты информации (ЗИ) и способы ее обеспечения. Системный метод при решении задач обеспечения комплексной защиты информации.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	2	ПК-14, ПК-15
	Итого	2	
3 Определение компонентов СИБ.	Правовая защита информации. Законодательная база по 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 съема 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	6	ПК-14, ПК-15

Согласована на портале № 40662

	предприятия. Организация системы охраны предприятия (физическая охрана, пожарная и охранная сигнализация, охранное телевидение, системы ограничения доступа). Организация аналитической работы по предупреждению утечки 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	6	
4 Технология определения и классификации состава и защищенности информации	Охраняемые сведения и объекты защиты.Особенности отнесения сведений, составляющих служебную, конфиденциальную и коммерческую тайну к различным степеням и категориям доступа	2	ПК-14, ПК-15
	Итого	2	
5 Построение СИБ телекоммуникационных систем на предприятии.	Разработка моделей СИБ ТКС. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования СИБ ТКС.Архитектурное построение комплексной системы защиты информации	5	ПК-14, ПК-15
	Итого	5	
6 Управление СИБ ТКС.	Структура и содержание технологии управления СИБ. Планирование и оперативное управление системой ЗИ, управление СИБ ТКС в условиях чрезвычайных ситуаций.Анализ надежности функционирования комплексной системы защиты информации.	2	ПК-14, ПК-15
	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.	2	ПК-14, ПК-15
	Итого	2	
8 Особенности управления СИБ ТКС в условиях чрезвычайных ситуаций	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 СИБ. Реорганизация и ликвидация СИБ. Определение должностного состава и численности СИБ. Планирование и отчетность о деятельности СИБ-Понимание рисков непрерывности и их влияние на	3	ПК-14, ПК-15

Согласована на портале № 40662

	цели деятельности организации и восстановление защитных мер СИБ ТКС.Восстановление после чрезвычайной ситуации функций и механизмов СИБ 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	3	
9 Состав методов и моделей оценки эффективности СИБ.	Основные термины и определения, характеризующие эффективность защиты информации. Содержание и особенности методологии оценки эффективности СИБ.Основные модели оценки эффективности СИБ.	2	ПК-14, ПК-15
	Итого	2	
Итого за семестр		26	

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 Основы информационной безопасности	+								
Последующие дисциплины									
1 Защита и обработка конфиденциальных документов		+		+	+		+	+	
2 Криптографические методы защиты информации		+	+		+	+		+	+
3 Организационное и правовое обеспечение информационной безопасности			+	+	+	+	+	+	
4 Организация и управление службой защиты информации на предприятии					+	+	+	+	+
5 Программно-аппаратные средства обеспечения информационной безопасности		+	+		+	+		+	+
6 Техническая защита информации		+	+		+	+		+	+

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.

Согласована на портале № 40662

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

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	КСР (КП/КР)	Сам. раб.	
ПК-14	+	+	+	+	Экзамен, Конспект самоподготовки, Опрос на занятиях, Консультирование, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию
ПК-15	+	+	+	+	Экзамен, Конспект самоподготовки, Опрос на занятиях, Консультирование, Выступление (доклад) на занятии, Тест, 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
5 семестр			
1 Введение	Сущность и понятие системы защиты информации с позиции системного подхода	4	ПК-14, ПК-15
	Итого	4	
2 Содержание и этапы проведения работ по организации систем информационной безопасности (СИБ) телекоммуникационных систем (ТКС) на предприятии.	Сущность и понятие объекта защиты информации, объекта информатизации	4	ПК-14, ПК-15
	Итого	4	
3 Определение компонентов СИБ.	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.	4	ПК-14, ПК-15

Согласована на портале № 40662

	Итого	4	
4 Технология определения и классификации состава и защищенности информации	Классификация защищаемых информационных ресурсов.	4	ПК-14, ПК-15
	Итого	4	
5 Построение СИБ телекоммуникационных систем на предприятии.	Помещения, предназначенные для конфиденциальных переговоров. ТКУИ, характерные для объекта защиты. Определения и понятия.Обработка защищаемой информации с использованием средств вычислительной техники. ТКУИ, характерные для объекта защиты. Определения и понятия.	4	ПК-14, ПК-15
	Итого	4	
6 Управление СИБ ТКС.	Модель угроз и нарушителя. Понятие и основные практические подходы к разработке.Аттестация объектов информатизации по требованиям безопасности информации.Основные понятия и особенности практической реализации. Состав примерного комплекта документов.	4	ПК-14, ПК-15
	Итого	4	
7 Служба защиты информации	Организация службы защиты информации (СлЗИ) и организационное проектирование деятельности СлЗИ.	4	ПК-14, ПК-15
	Итого	4	
8 Особенности управления СИБ ТКС в условиях чрезвычайных ситуаций	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 СИБ ТКС.	4	ПК-14, ПК-15
	Итого	4	
9 Состав методов и моделей оценки эффективности СИБ.	Содержание и особенности методологии оценки эффективности СИБ. Основные модели оценки эффективности СИБ.	4	ПК-14, ПК-15
	Итого	4	
Итого за семестр		36	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
5 семестр				

Согласована на портале № 40662

1 Введение	Подготовка к практическим занятиям, семинарам	1	ПК-14, ПК-15	Конспект самоподготовки, Опрос на занятиях, Тест
	Итого	1		
2 Содержание и этапы проведения работ по организации систем информационной безопасности (СИБ) телекоммуникационных систем (ТКС) на предприятии.	Подготовка к практическим занятиям, семинарам	5	ПК-14, ПК-15	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Итого	5		
3 Определение компонентов СИБ.	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-15	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Итого	4		
4 Технология определения и классификации состава и защищенности информации	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-15	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Итого	4		
5 Построение СИБ телекоммуникационных систем на предприятии.	Подготовка к практическим занятиям, семинарам	5	ПК-14, ПК-15	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Итого	5		
6 Управление СИБ ТКС.	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-15	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Итого	4		
7 Служба защиты информации	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-15	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Итого	4		
8 Особенности управления СИБ ТКС в условиях чрезвычайных ситуаций	Подготовка к практическим занятиям, семинарам	5	ПК-14, ПК-15	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Итого	5		
9 Состав методов и моделей оценки эффективности СИБ.	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-15	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию, Тест
	Итого	4		
Итого за семестр		36		
	Подготовка и сдача экзамена	36		Экзамен

Согласована на портале № 40662

Итого	72		

10. Курсовой проект / курсовая работа

Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсового проекта / курсовой работы представлены таблице 10.1.

Таблица 10.1 – Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсового проекта / курсовой работы

Наименование аудиторных занятий	Трудоемкость, ч	Формируемые компетенции
5 семестр		
Определение компонентов СИБ.	2	ПК-14, ПК-15
Построение СИБ телекоммуникационных систем на предприятии.	2	
Служба защиты информации.	2	
Особенностей управления СИБ ТКС в условиях чрезвычайных ситуаций.	2	
Состав методов и моделей оценки эффективности СИБ.	2	
Итого за семестр	10	

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
5 семестр				
Выступление (доклад) на занятии	5	3	7	15
Конспект самоподготовки	3	3	3	9
Опрос на занятиях	5	3	7	15
Отчет по практическому занятию	4	3	4	11
Тест	5	5	10	20
Итого максимум за период	22	17	31	70
Экзамен				30
Нарастающим итогом	22	39	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 № 40662

≥ 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: 25.07.2018).

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: 25.07.2018).

2. "Модель системы защиты информации на предприятии" Материалы одиннадцатой международной научно-практическая конференции «Электронные средства и системы управления», Томск, ТУСУР, 25-27 ноября 2015 года, в двух частях, часть 2 [Электронный ресурс]: - Режим доступа: http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/conferences/archive/2015-2.pdf (дата обращения: 25.07.2018).

3. "Модель угроз подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров" Материалы одиннадцатой международной научно-практическая конференции «Электронные средства и системы управления», Томск, ТУСУР, 25-27 ноября 2015 года, в двух частях, часть 2 [Электронный ресурс]: - Режим доступа: http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/conferences/archive/2015-2.pdf (дата обращения: 25.07.2018).

4. "Модель уязвимостей системы обеспечения информационной безопасности на предприятии" Материалы одиннадцатой международной научно-практическая конференции «Электронные средства и системы управления», Томск, ТУСУР, 25-27 ноября 2015 года, в двух частях, часть 2 [Электронный ресурс]: - Режим доступа: http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/conferences/archive/2015-2.pdf (дата обращения: 25.07.2018).

Согласована на портале № 40662

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: 25.07.2018).

2. Информационные технологии в управлении качеством и защита информации [Электронный ресурс]: Методические рекомендации к курсовым работам и организации самостоятельной работы студентов / Е. Г. Годенова - 2011. 35 с. - Режим доступа: https://edu.tusur.ru/publications/290 (дата обращения: 25.07.2018).

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

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.);

Согласована на портале № 40662

- 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 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** исполь-

Согласована на портале № 40662

зуются 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. Информация это -
1) сведения, поступающие от СМИ
2) только документированные сведения о лицах, предметах, фактах, событиях
3) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
4) только сведения, содержащиеся в электронных базах данных

2. Информация
1) не исчезает при потреблении
2) становится доступной, если она содержится на материальном носителе
3) подвергается только "моральному износу"
4) характеризуется всеми перечисленными свойствами

3. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
1) достоверной
2) конфиденциальной
3) документированной
4) коммерческой тайной

4. Формы защиты интеллектуальной собственности -
1) авторское, патентное право и коммерческая тайна
2) интеллектуальное право и смежные права
3) коммерческая и государственная тайна
4) гражданское и административное право

5. По принадлежности информационные ресурсы подразделяются на
1) государственные, коммерческие и личные
2) государственные, не государственные и информацию о гражданах
3) информацию юридических и физических лиц
4) официальные, гражданские и коммерческие

6. К негосударственным относятся информационные ресурсы
1) созданные, приобретенные за счет негосударственных учреждений и организаций
2) созданные, приобретенные за счет негосударственных предприятий и физических лиц
3) полученные в результате дарения юридическими или физическими лицами
4) все указанное в пунктах 1-3

8. По доступности информация классифицируется на
1) открытую информацию и государственную тайну
2) конфиденциальную информацию и информацию свободного доступа
3) информацию с ограниченным доступом и общедоступную информацию
4) виды информации, указанные в остальных пунктах

Согласована на портале № 40662

9. К конфиденциальной информации относятся документы, содержащие
1) государственную тайну
2) законодательные акты
3) "ноу-хау"
4) сведения о золотом запасе страны

10. Запрещено относить к информации ограниченного доступа
1) информацию о чрезвычайных ситуациях
2) информацию о деятельности органов государственной власти
3) документы открытых архивов и библиотек
4) все, перечисленное в остальных пунктах

11. К конфиденциальной информации не относится
1) коммерческая тайна
2) персональные данные о гражданах
3) государственная тайна
4) "ноу-хау"

12. Вопросы информационного обмена регулируются (...) правом
1) гражданским
2) информационным
3) конституционным
4) уголовным

13. Согласно ст.132 ГК РФ интеллектуальная собственность это
1) информация, полученная в результате интеллектуальной деятельности индивида
2) литературные, художественные и научные произведения
3) изобретения, открытия, промышленные образцы и товарные знаки
4) исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности

14. Интеллектуальная собственность включает права, относящиеся к
1) литературным, художественным и научным произведениям, изобретениям и открытиям
2) исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
3) промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям
4) всему, указанному в остальных пунктах

15. Конфиденциальная информация это
1) сведения, составляющие государственную тайну
2) сведения о состоянии здоровья высших должностных лиц
3) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
4) данные о состоянии преступности в стране

16. Какая информация подлежит защите?
1) информация, циркулирующая в системах и сетях связи
2) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
3) только информация, составляющая государственные информационные ресурсы
4) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

17. Система защиты государственных секретов определяется Законом

Согласована на портале № 40662

1) "Об информации, информатизации и защите информации"
2) "Об органах ФСБ"
3) "О государственной тайне"
4) "О безопасности"

18. Государственные информационные ресурсы не могут принадлежать
1) физическим лицам
2) коммерческим предприятиям
3) негосударственным учреждениям
4) всем перечисленным субъектам

19. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает
1) Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"
2) ГК РФ
3) Закон "Об информации, информатизации и защите информации"
4) Конституция

20. Классификация и виды информационных ресурсов определены
1) Законом "Об информации, информатизации и защите информации"
2) Гражданским кодексом
3) Конституцией
4) всеми документами, перечисленными в остальных пунктах

14.1.2. Экзаменационные вопросы

1. Сущность и понятие системы защиты информации с позиции системного подхода
2. Сущность и понятие объекта защиты информации, объекта информатизации
3. Сущность и понятие объекта защиты информации, объекта информатизации.
4. Определение, понятие и физический смысл технического канала утечки информации (ТКУИ).
5. Методология защиты информации от утечки по техническим каналам.
6. Классификация защищаемых информационных ресурсов.
7. Помещения, предназначенные для конфиденциальных переговоров.
8. ТКУИ, характерные для объекта защиты. Определения и понятия.
9. Обработка защищаемой информации с использованием средств вычислительной техники.
10. ТКУИ, характерные для объекта защиты. Определения и понятия.
11. Модель угроз и нарушителя.
12. Понятие и основные практические подходы к разработке.
13. Аттестация объектов информатизации по требованиям безопасности информации.
14. Основные понятия и особенности практической реализации.
15. Состав примерного комплекта документов.
16. Организация службы защиты информации (СлЗИ) и организационное проектирование деятельности СлЗИ.
17. Определение и понятие чрезвычайной ситуации.
18. Аспекты обеспечения условий непрерывности в информационной сфере организации.
19. Роль совета директоров и исполнительных органов организации.
20. Идентификация недостатков.
21. Непрерывность сервисов в изменяющейся среде и обеспечение СИБ ТКС.
22. Содержание и особенности методологии оценки эффективности СИБ.
23. Основные модели оценки эффективности СИБ.

14.1.3. Темы докладов

1.Содержание и этапы проведения работ по организации систем информационной безопасности (СИБ) телекоммуникационных систем (ТКС) на предприятии.
2.Определение компонентов СИБ.

Согласована на портале № 40662

3.Технология определения и классификации состава и защищенности информации

4. Построение СИБ телекоммуникационных систем на предприятии.

5.Управление СИБ ТКС.

6. Служба защиты информации

7. Особенности управления СИБ ТКС в условиях чрезвычайных ситуаций

8. Состав методов и моделей оценки эффективности СИБ.

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 системой информационной безопасности телекоммуникационных систем на предприятии. Специфика курса.

Цели комплексной защиты информации (ЗИ) и способы ее обеспечения. Системный метод при решении задач обеспечения комплексной защиты информации.

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 по 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 съема 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 утечки 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 и коммерческую тайну к различным степеням и категориям доступа

Разработка моделей СИБ ТКС. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования СИБ ТКС.

Архитектурное построение комплексной системы защиты информации

Структура и содержание технологии управления СИБ. Планирование и оперативное управление системой ЗИ, управление СИБ ТКС в условиях чрезвычайных ситуаций.

Анализ надежности функционирования комплексной системы защиты информации.

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 СИБ. Реорганизация и ликвидация СИБ. Определение должностного состава и численности СИБ. Планирование и отчетность о деятельности СИБ

Согласована на портале № 40662

Понимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер СИБ ТКС.

Восстановление после чрезвычайной ситуации функций и механизмов СИБ 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.

Основные термины и определения, характеризующие эффективность защиты информации. Содержание и особенности методологии оценки эффективности СИБ.

Основные модели оценки эффективности СИБ.

14.1.5. Вопросы на самоподготовку

1.Содержание и этапы проведения работ по организации систем информационной безопасности (СИБ) телекоммуникационных систем (ТКС) на предприятии.

2.Определение компонентов СИБ.

3.Технология определения и классификации состава и защищенности информации

4. Построение СИБ телекоммуникационных систем на предприятии.

5.Управление СИБ ТКС.

6. Служба защиты информации

7. Особенностей управления СИБ ТКС в условиях чрезвычайных ситуаций

8. Состав методов и моделей оценки эффективности СИБ.

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

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.

Классификация защищаемых информационных ресурсов.

Помещения, предназначенные для конфиденциальных переговоров. ТКУИ, характерные для объекта защиты. Определения и понятия.

Обработка защищаемой информации с использованием средств вычислительной техники. ТКУИ, характерные для объекта защиты. Определения и понятия.

Модель угроз и нарушителя. Понятие и основные практические подходы к разработке.

Аттестация объектов информатизации по требованиям безопасности информации.

Основные понятия и особенности практической реализации. Состав примерного комплекта документов.

Организация службы защиты информации (СлЗИ) и организационное проектирование деятельности СлЗИ.

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 СИБ ТКС.

Содержание и особенности методологии оценки эффективности СИБ. Основные модели оценки эффективности СИБ.

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,	Преимущественно письменная проверка

Согласована на портале № 40662

	контрольные работы	
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 № 40662