МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Принципы построения систем информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль): **Безопасность телекоммуникационных систем информационного взаимодействия**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
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	Из них в интерактивной форме	7	7	часов
6	Самостоятельная работа	36	36	часов
7	Всего (без экзамена)	108	108	часов
8	Подготовка и сдача экзамена	36	36	часов
9	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е

Экзамен: 5 семестр

Томск 2017

Согласована на портале № 21493

Рассмотрена и одобрена на заседании кафедры
протокол № 1 от « 7 » 6 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа 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 ноября 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент каф. РЗИ _____ А. П. Кшнянкин

Заведующий обеспечивающей каф. РЗИ _____ А. В. Фатеев

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф. РЗИ _____ А. В. Фатеев

Эксперт:

ведущий инженер каф. РЗИ РТФ _____ Ю. В. Зеленецкая

Согласована на портале № 21493

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 следующие дисциплины: Основы информационной безопасности.

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

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 студент 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 № 21493

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
Из них в интерактивной форме	7	7
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	Лекции	Практические занятия	Самостоятельная работа	Курсовая работа	Всего часов (без экзамена)	Формируемые компетенции
5 семестр						
1 Введение	2	4	1	10	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

Согласована на портале № 21493

7 Служба защиты информации	2	4	4		10	ПК-14, ПК-15
8 Особенностей управления СИБ ТКС в условиях чрезвычайных ситуаций	3	4	5		12	ПК-14, ПК-15
9 Состав методов и моделей оценки эффективности СИБ.	2	4	4		10	ПК-14, ПК-15
Итого за семестр	26	36	36	10	108	
Итого	26	36	36	10	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 ин-формации. Выбор методов и средств защиты ин-формации	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 информа-	6	ПК-14, ПК-15

Согласована на портале № 21493

	ции. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты и их классификация. Каналы утечки информации (оптический, акустический, радиоэлек-тронный). Методы защиты от несанкционирован-ного 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.		
	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. Пла-нирование и	2	ПК-14, ПК-15

Согласована на портале № 21493

	оперативное управление системой ЗИ, управление СИБ ТКС в условиях чрезвычайных ситуаций.Анализ надежности функционирования комплексной системы защиты информации.		
	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 Особенностей 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 СИБПонимание 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.	3	ПК-14, ПК-15
	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	

Согласована на портале № 21493

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

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 и видов занятий, формируемых при изучении дисциплины

	Виды занятий	Формы контроля

Согласована на портале № 21493

Компетенции	Лекции	Практические занятия	Контроль самостоятельной работы (курсовой проект / курсовая работа)	Самостоятельная работа	
ПК-14	+	+	+	+	Экзамен, Конспект самоподготовки, Защита отчета, Опрос на занятиях, Выступление (доклад) на занятии, Отчет по практическому занятию
ПК-15	+	+	+	+	Экзамен, Конспект самоподготовки, Защита отчета, Опрос на занятиях, Выступление (доклад) на занятии, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные лекции	Всего
5 семестр		
Мозговой штурм	1	1
Решение ситуационных задач	1	1
Презентации с использованием видеофильмов с обсуждением	4	4
Выступление студента в роли обучающего	1	1

Согласована на портале № 21493

Итого за семестр:	7	7
Итого	7	7

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
	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.Основнае понятия и осо-	4	ПК-14, ПК-15

Согласована на портале № 21493

	бенности практической реализации. Состав примерного комплекта документов.		
	Итого	4	
7 Служба защиты информации	Организация службы защиты информации (СлЗИ) и организационное проектирование деятельности СлЗИ.	4	ПК-14, ПК-15
	Итого	4	
8 Особенностей 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				
1 Введение	Подготовка к практическим занятиям, семинарам	1	ПК-14, ПК-15	Конспект самоподготовки, Опрос на занятиях
	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	Конспект самоподготовки, Опрос на занятиях
	Итого	5		
3 Определение компонентов СИБ.	Подготовка к практическим занятиям, семина-	4	ПК-14, ПК-15	Конспект самоподготовки, Опрос на занятиях

Согласована на портале № 21493

	рам			
	Итого	4		
4 Технология определения и классификации состава и защищенности информации	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-15	Конспект самоподготовки, Опрос на занятиях
	Итого	4		
5 Построение СИБ телекоммуникационных систем на предприятии.	Подготовка к практическим занятиям, семинарам	5	ПК-14, ПК-15	Конспект самоподготовки, Опрос на занятиях
	Итого	5		
6 Управление СИБ ТКС.	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-15	Конспект самоподготовки, Опрос на занятиях
	Итого	4		
7 Служба защиты информации	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-15	Конспект самоподготовки, Опрос на занятиях
	Итого	4		
8 Особенностей управления СИБ ТКС в условиях чрезвычайных ситуаций	Подготовка к практическим занятиям, семинарам	5	ПК-14, ПК-15	Конспект самоподготовки, Опрос на занятиях
	Итого	5		
9 Состав методов и моделей оценки эффективности СИБ.	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-15	Конспект самоподготовки, Опрос на занятиях
	Итого	4		
Итого за семестр		36		
	Подготовка и сдача экзамена	36		Экзамен
Итого		72		

10. Курсовая работа (проект)

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

Таблица 10. 1 – Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсовой работы (проекта)

Наименование аудиторных занятий	Трудоемкость, ч	Формируемые компетенции
5 семестр		
Определение компонентов СИБ.	2	ПК-14, ПК-15
Построение СИБ телекоммуникационных систем на предприятии.	2	

Согласована на портале № 21493

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 студентов

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
Защита отчета	5	7	9	21
Конспект самоподготовки	3	3	3	9
Опрос на занятиях	5	3	7	15
Отчет по практическому занятию	4	2	4	10
Итого максимум за период	22	18	30	70
Экзамен				30
Нарастающим итогом	22	40	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)

Согласована на портале № 21493

	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: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5262, дата обращения: 07.06.2017.

12.2. Дополнительная литература

1. Защита информации от утечки по техническим каналам: Учебное пособие / Голиков А. М. - 2015. 256 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5263, дата обращения: 07.06.2017.
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]. - http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/conferences/archive/2015-2.pdf
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]. - http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/conferences/archive/2015-2.pdf
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]. - http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/conferences/archive/2015-2.pdf

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информации в инфокоммуникационных системых и сетях: Учебное пособие для практических и семинарских занятий (Часть 1) / Голиков А. М. - 2015. 103 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5330, дата обращения: 07.06.2017.
2. Информационные технологии в управлении качеством и защита информации: Методические рекомендации к курсовым работам и организации самостоятельной работы студентов / Годенова Е. Г. - 2011. 35 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/290, дата обращения: 07.06.2017.

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа 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.

Согласована на портале № 21493

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. 1.Сайт кафедры РЗИ на образовательном портале ТУСУРа;
2. 2. Локальная сеть кафедры РЗИ: Students\Фамилия преподавателя\ Название файла.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Лекционные, практические и лабораторные занятия проводятся в специализированных аудиториях кафедры РЗИ. 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 наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебные аудитории, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 407, 412, 416. Состав оборудования: Учебная мебель; Доска магнитно-маркерная -1шт.; Коммутатор D-Link Switch 24 port - 1шт.; Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. -14 шт. Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3/Microsoft Windows 7 Professional with SP1; Microsoft Windows Server 2008 R2; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft Office Access 2003; VirtualBox 6.2. Имеется помещения для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 4 этаж, ауд. 407,412, 416. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **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 удаленного просмотра.

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

Объём часов, предусмотренных учебным планом для изучения дисциплины, по-зволяет

Согласована на портале № 21493

осветить только наиболее важные моменты и раскрыть базовые понятия при чтении лекций. Поэтому при реализации программы студенты должны работать самостоятельно как при повторении лекционного материала, так и при подготовке к лабораторным и практическим занятиям, к разработке курсового проекта. Для обеспечения эффектив¬ного усвоения студентами материалов дисциплины необходимо на первом занятии познакомить их с основными положениями и требованиями рабочей программы, с подлежащими изучению темами, списком основной и дополнительной литературы, с положениями балльно-рейтинговой системы оценки успеваемости. На лекциях необходимо обращать внимание на особенности применения рассматриваемого материала в последующих курсах, а также в будущей профессиональной деятельности. В учебном процессе следует применять интерактивные методы обучения для увеличения заинтересованности студентов и повышения их компетенций.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	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 средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов 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 инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

Согласована на портале № 21493

– 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 обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 21493

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Принципы построения систем информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль): **Безопасность телекоммуникационных систем информационного взаимодействия**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **3**
Семестр: **5**

Учебный план набора 2012 года

Разработчик:
- доцент каф. РЗИ А. П. Кшнянкин

Экзамен: 5 семестр

Томск 2017

Согласована на портале № 21493

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования 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	Должен знать • основы организации и управления системой информационной безопасности телекоммуникационных систем на предприятии. ; Должен уметь • на концептуальном и практическом уровне разрабатывать и внедрять системы информационной безопасности телекоммуникационных систем на предприятии. ; Должен владеть • навыками внедрения систем информационной безопасности телекоммуникационных систем на предприятии. ;
ПК-15	способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания	

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПК-14

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.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Согласована на портале № 21493

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	основы организации и управления системой информационной безопасности телекоммуникационных систем на предприятии.	на концептуальном и практическом уровне разрабатывать и внедрять системы информационной безопасности телекоммуникационных систем на предприятии.	навыками внедрения систем информационной безопасности телекоммуникационных систем на предприятии.
Виды занятий	• Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Конспект самоподготовки; • Опрос на занятиях; • Выступление (доклад) на занятии; • Отчет по практическому занятию; • Экзамен;	• Конспект самоподготовки; • Опрос на занятиях; • Выступление (доклад) на занятии; • Отчет по практическому занятию; • Экзамен;	• Выступление (доклад) на занятии; • Отчет по практическому занятию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости;	• Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем;	• Контролирует работу, проводит оценку, совершенствует действия работы;
Хорошо (базовый уровень)	• Знает факты, принципы, процессы, общие понятия в пределах изучаемой области;	• Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования ;	• Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем ;
Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями;	• Обладает основными умениями, требуемыми для выполнения простых задач;	• Работает при прямом наблюдении;

Согласована на портале № 21493

2.2 Компетенция ПК-15

ПК-15: способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	основы организации и управления системой информационной безопасности телекоммуникационных систем на предприятии.	на концептуальном и практическом уровне разрабатывать и внедрять системы информационной безопасности телекоммуникационных систем на предприятии.	навыками внедрения систем информационной безопасности телекоммуникационных систем на предприятии.
Виды занятий	• Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Конспект самоподготовки; • Опрос на занятиях; • Выступление (доклад) на занятии; • Отчет по практическому занятию; • Экзамен;	• Конспект самоподготовки; • Опрос на занятиях; • Выступление (доклад) на занятии; • Отчет по практическому занятию; • Экзамен;	• Выступление (доклад) на занятии; • Отчет по практическому занятию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости;	• Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем;	• Контролирует работу, проводит оценку, совершенствует действия работы;
Хорошо (базовый уровень)	• Знает факты, принципы, процессы, общие понятия в пределах изучаемой области;	• Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования ;	• Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем ;

Согласована на портале № 21493

Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями;	• Обладает основными умениями, требуемыми для выполнения простых задач;	• Работает при прямом наблюдении;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 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.

3.2 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 ин-формации. Выбор методов и средств защиты ин-формации
- 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, радиоэлек-тронный). Методы защиты от несанкционирован-ного 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 ком-

Согласована на портале № 21493

мерческую 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. Пла-нирование 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

– 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.

3.3 Темы докладов

– 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.

3.4 Экзаменационные вопросы

– 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. Основнае 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.

Согласована на портале № 21493

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

3.5 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.
– Основнае 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.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5262, свободный.

4.2. Дополнительная литература

1. Защита информации от утечки по техническим каналам: Учебное пособие / Голиков А. М. - 2015. 256 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5263, свободный.
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]. - http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/conferences/archive/2015-2.pdf
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]. - http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/conferences/archive/2015-2.pdf
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

Согласована на портале № 21493

[Электронный ресурс]. - http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/conferences/archive/2015-2.pdf

4.3. Обязательные учебно-методические пособия

1. Защита информации в инфокоммуникационных системых и сетях: Учебное пособие для практических и семинарских занятий (Часть 1) / Голиков А. М. - 2015. 103 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5330, свободный.
2. Информационные технологии в управлении качеством и защита информации: Методические рекомендации к курсовым работам и организации самостоятельной работы студентов / Годенова Е. Г. - 2011. 35 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/290, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. 1.Сайт кафедры РЗИ на образовательном портале ТУСУРа;
2. 2. Локальная сеть кафедры РЗИ: Students\Фамилия преподавателя\ Название файла.

Согласована на портале № 21493