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

Техническая защита информации

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: **4, 5**
Семестр: **8, 9**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	9 семестр	Всего	Единицы
1	Лекции	36		36	часов
2	Практические занятия	32	40	72	часов
3	Лабораторные работы	22		22	часов
4	Контроль самостоятельной работы (курсовой проект / курсовая работа)		10	10	часов
5	Всего аудиторных занятий	90	50	140	часов
6	Из них в интерактивной форме	23		23	часов
7	Самостоятельная работа	54	22	76	часов
8	Всего (без экзамена)	144	72	216	часов
9	Подготовка и сдача экзамена	36		36	часов
10	Общая трудоемкость	180	72	252	часов
		5.0	2.0	7.0	З.Е

Экзамен: 8 семестр
Зачет: 9 семестр
Курсовая работа (проект): 9 семестр

Согласована на портале № 19518

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 3 » 5 2017 г.

Томск 2017

Согласована на портале № 19518

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:

преподаватель каф. РЗИ _____ А. В. Максимов

Заведующий обеспечивающей каф. РЗИ _____ А. С. Задорин

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

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф. РЗИ _____ А. С. Задорин

Эксперт:

Доцент ТУСУР каф.РЗИ _____ А. П. Кшнянкин

Согласована на портале № 19518

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью изучения дисциплины является ознакомление студентов с различными видами угроз информационным ресурсам, каналами утечки информации,

способами и средствами защиты конфиденциальной информации техническими средствами.

1.2. Задачи дисциплины

– Задачами изучения дисциплины являются: изучение технических средств добывания информации;

– назначения и функций видов разведки;

– способов доступа к источникам конфиденциальной информации без проникновения на объект защиты;

– способов и средств защиты конфиденциальной информации техническими средствами.

2. Место дисциплины в структуре ОПОП

Дисциплина «Техническая защита информации» (Б1.Б.18) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Дискретная математика, Иностранный язык, Информатика, Информационные технологии, Математический анализ, Русский язык и культура речи, Теория вероятностей и математическая статистика.

Последующими дисциплинами являются: Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

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

– ПК-13 способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем;

В результате изучения дисциплины студент должен:

– **знать** технические каналы утечки информации; возможности технических разведок; способы и средства защиты информации от утечки по техническим каналам; методы и средства контроля эффективности технической защиты информации.

– **уметь** анализировать и оценивать угрозы информационной безопасности объекта.

– **владеть** методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 7.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		8 семестр	9 семестр
Аудиторные занятия (всего)	140	90	50
Лекции	36	36	
Практические занятия	72	32	40
Лабораторные работы	22	22	

Согласована на портале № 19518

Контроль самостоятельной работы (курсовой проект / курсовая работа)	10		10
Из них в интерактивной форме	23	23	
Самостоятельная работа (всего)	76	54	22
Выполнение расчетных работ	6	6	
Выполнение индивидуальных заданий	4	4	
Оформление отчетов по лабораторным работам	12	12	
Проработка лекционного материала	8	8	
Подготовка к практическим занятиям, семинарам	46	24	22
Всего (без экзамена)	216	144	72
Подготовка и сдача экзамена	36	36	
Общая трудоемкость ч	252	180	72
Зачетные Единицы	7.0	5.0	2.0

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	Лабораторные работы	Самостоятельная работа	Курсовая работа	Всего часов (без экзамена)	Формируемые компетенции
8 семестр							
1 Технические средства добывания информации.	8	8	4	10	0	30	ПК-13, ПК-6
2 Принципы оптической, радиоэлектронной, акустической разведок.	10	8	0	8	0	26	ПК-13, ПК-6
3 Способы и средства технической защиты конфиденциальной информации.	8	6	6	12	0	32	ПК-13, ПК-6
4 Способы доступа к источникам конфиденциальной информации без нарушения государственной границы.	4	0	0	4	0	8	ПК-13, ПК-6
5 Организация работ по технической защите на предприятиях и учреждениях.	6	10	12	20	0	48	ПК-13, ПК-6
Итого за семестр	36	32	22	54	0	144	
9 семестр							
6 Практические и самостоятельные	0	40	0	22	10	62	ПК-13, ПК-6

Согласована на портале № 19518

занятия							
Итого за семестр	0	40	0	22	10	72	
Итого	36	72	22	76	10	216	

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
8 семестр			
1 Технические средства добывания информации.	Характеристика средств технической разведки. Структура системы технической разведки. Силы и средства системы технической разведки. Возможности средств технической разведки.	8	ПК-6
	Итого	8	
2 Принципы оптической, радиоэлектронной, акустической разведок.	Средства наблюдения в оптическом диапазоне. Оптические системы. Визуально-оптические приборы. Фото- и киноаппараты. Средства телевизионного наблюдения. Средства наблюдения в инфракрасном диапазоне. Средства наблюдения в радиодиапазоне	10	ПК-6
	Итого	10	
3 Способы и средства технической защиты конфиденциальной информации.	Структурное скрытие речевой информации в каналах связи. Средства противодействия наблюдению в оптическом диапазоне. Средства звукоизоляции и звукопоглощения акустического сигнала. Средства предотвращения утечки информации с помощью закладных подслушивающих устройств. Средства предотвращения утечки информации через ПЭМИН.	8	ПК-6
	Итого	8	
4 Способы доступа к источникам конфиденциальной информации без нарушения государственной границы.	Пространственное, энергетическое и временное условия разведывательного контакта. Способы несанкционированного доступа к информации. Виды носителей, распространяющихся за пределы контролируемой зоны, за пределы государственной границы	4	ПК-6

Согласована на портале № 19518

	Итого	4	
5 Организация работ по технической защите на предприятиях и учреждениях.	Задачи и структура государственной системы инженерно-технической защиты информации. Нормативно-правовая база инженерно-технической защиты информации. Организация инженерно-технической защиты информации на предприятиях и учреждениях государственных и коммерческих структур. Контроль эффективности инженерно-технической защиты информации	6	ПК-6
	Итого	6	
Итого за семестр		36	
Итого		36	

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

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

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин					
	1	2	3	4	5	6
Предшествующие дисциплины						
1 Дискретная математика	+	+	+	+	+	
2 Иностранный язык	+	+	+	+	+	
3 Информатика	+	+	+	+	+	
4 Информационные технологии	+	+	+	+	+	
5 Математический анализ	+	+	+	+	+	
6 Русский язык и культура речи	+	+	+	+	+	
7 Теория вероятностей и математическая статистика	+	+	+	+	+	
Последующие дисциплины						
1 Преддипломная практика	+	+	+	+	+	

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Согласована на портале № 19518

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

Компетенции	Виды занятий					Формы контроля
	Лекции	Практические занятия	Лабораторные работы	Контроль самостоятельной работы (курсовой проект / курсовая работа)	Самостоятельная работа	
ПК-6	+	+	+	+	+	Контрольная работа, Отчет по индивидуальному заданию, Экзамен, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов (работ), Отчет по курсовой работе, Отчет по практическому занятию
ПК-13		+	+		+	Контрольная работа, Отчет по индивидуальному заданию, Экзамен, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов (работ), Отчет по курсовой работе, 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 практические занятия	Интерактивные лабораторные занятия	Интерактивные лекции	Всего
8 семестр				
Выступление студента в роли обучающего	8	6	9	23
Итого за семестр:	8	6	9	23
9 семестр				

Согласована на портале № 19518

Разработка проекта				0
Итого за семестр:	0	0	0	0
Итого	8	6	9	23

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Технические средства добывания информации.	Экспериментальное исследование характеристик телефонных линий с помощью локатора-рефлектометра "ОТКЛИК-2"	4	ПК-6
	Итого	4	
3 Способы и средства технической защиты конфиденциальной информации.	Экспериментальное исследование защищенности помещений от утечки речевой информации по виброакустическому каналу.	2	ПК-13, ПК-6
	Обнаружение полупроводниковых элементов с помощью нелинейного локатора «КАТРАН»	4	
	Итого	6	
5 Организация работ по технической защите на предприятиях и учреждениях.	Экспериментальное исследование защищенности помещений от утечки информации по по электромагнитному каналу, с помощью спектроанализатора и антенн электромагнитного поля	4	ПК-13, ПК-6
	Экспериментальное исследование защищенности помещений от утечки информации по по электромагнитному каналу, с помощью сканирующего приемника электромагнитного поля и управляющей программы "ФИЛИН"	4	
	Комплексное исследование защищенности помещений от утечек речевой информации по всем каналам с помощью набора "Пиранья".	4	
	Итого	12	
Итого за семестр		22	
Итого		22	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Согласована на портале № 19518

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Технические средства добывания информации.	Расчет характеристик акустического канала утечки информации по акустическим волноводам и отверстиям электропроводки в строительных конструкциях.	8	ПК-6
	Итого	8	
2 Принципы оптической, радиоэлектронной, акустической разведок.	Расчет характеристик виброакустического канала утечки информации по трубам отопления и водоснабжения.	8	ПК-6
	Итого	8	
3 Способы и средства технической защиты конфиденциальной информации.	Расчет гармонических составляющих второго и третьего порядка, образующихся на нелинейных элементах и окисленных металлических предметах.	6	ПК-6
	Итого	6	
5 Организация работ по технической защите на предприятиях и учреждениях.	Расчет времени задержки отраженного сигнала в линии связи при отражении от неоднородности	10	ПК-6
	Итого	10	
Итого за семестр		32	
9 семестр			
6 Практические и самостоятельные занятия	Измерение ПЭМИН от различных мониторов и расчет возможности приема ПЭМИН на границе контролируемой зоны	12	ПК-13, ПК-6
	Анализ возможности подавления цифровых диктофонов, расчет уровня требуемой мощности.	12	
	Определение диаграммы направленности антенного устройства нелинейного локатора	8	
	Анализ и расчет ПЭМИН от импульсного источника питания акустической системы конференцзала	8	
	Итого	40	

Согласована на портале № 19518

Итого за семестр		40	
Итого		72	

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
8 семестр				
1 Технические средства добывания информации.	Подготовка к практическим занятиям, семинарам	6	ПК-13, ПК-6	Защита курсовых проектов (работ), Защита отчета, Опрос на занятиях, Отчет по курсовой работе, Отчет по лабораторной работе, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	2		
	Итого	10		
2 Принципы оптической, радиоэлектронной, акустической разведок.	Подготовка к практическим занятиям, семинарам	6	ПК-13, ПК-6	Опрос на занятиях, Экзамен
	Проработка лекционного материала	2		
	Итого	8		
3 Способы и средства технической защиты конфиденциальной информации.	Подготовка к практическим занятиям, семинарам	6	ПК-13, ПК-6	Контрольная работа, Отчет по лабораторной работе, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	2		
	Оформление отчетов по лабораторным работам	2		
	Итого	12		
4 Способы доступа к источникам конфиденциальной информации без нарушения государственной границы.	Выполнение индивидуальных заданий	4	ПК-13, ПК-6	Экзамен
	Итого	4		
5 Организация работ по технической защите на предприятиях и	Подготовка к практическим занятиям, семинарам	6	ПК-13, ПК-6	Защита отчета, Опрос на занятиях, Отчет по индивидуальному

Согласована на портале № 19518

учреждениях.	Проработка лекционного материала	2		заданию, Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	2		
	Оформление отчетов по лабораторным работам	2		
	Оформление отчетов по лабораторным работам	2		
	Выполнение расчетных работ	6		
	Итого	20		
Итого за семестр		54		
	Подготовка и сдача экзамена	36		Экзамен
9 семестр				
6 Практические и самостоятельные занятия	Подготовка к практическим занятиям, семинарам	6	ПК-13, ПК-6	Опрос на занятиях
	Подготовка к практическим занятиям, семинарам	4		
	Подготовка к практическим занятиям, семинарам	6		
	Подготовка к практическим занятиям, семинарам	6		
	Итого	22		
Итого за семестр		22		
Итого		112		

9.1. Вопросы для подготовки к практическим занятиям, семинарам

1. Проработка программы для исследования ПЭМИН
2. Измерение ПЭМИН от различных мониторов и расчет возможности приема ПЭМИН на границе контролируемой зоны
3. Измерение ПЭМИН от различных мониторов и расчет возможности приема ПЭМИН на границе контролируемой зоны

10. Курсовая работа (проект)

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

Согласована на портале № 19518

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

Наименование аудиторных занятий	Трудоемкость, ч	Формируемые компетенции
9 семестр		
□ Теоретические аспекты методов контроля периметра. □ Теоретические предпосылки разработки СВЧ подавителя радиозакладок и диктофонов. □ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в радиорелейных системах связи, с цифровыми видами модуляции(QPSK,KAM16-256).□ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах связи с WI-Fi.□ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах широкополосного доступа,WIMAX.□ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах связи с ISDN.□ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах связи с ADSL	10	ПК-6
Итого за семестр	10	

10.1 Темы курсовых работ

Примерная тематика курсовых работ (проектов):

– □ Теоретические аспекты методов контроля периметра

– □ Теоретические предпосылки разработки СВЧ подавителя радиозакладок и диктофонов.

– □ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в радиорелейных системах связи, с цифровыми видами модуляции(QPSK,KAM16-256)

– □ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах связи с WI-Fi

– □ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах широкополосного доступа,WIMAX

– □ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах связи с ISDN

– □ Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах связи с ADSL

Согласована на портале № 19518

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
8 семестр				
Защита курсовых проектов (работ)	5	5	5	15
Защита отчета	4	5	5	14
Контрольная работа	2	2	2	6
Опрос на занятиях	3	3	3	9
Отчет по курсовой работе	4	5	5	14
Отчет по лабораторной работе	4	4	4	12
Итого максимум за период	22	24	24	70
Экзамен				30
Нарастающим итогом	22	46	70	100
9 семестр				
Защита курсовых проектов (работ)	30	20	50	100
Итого максимум за период	30	20	50	100
Нарастающим итогом	30	50	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)

Согласована на портале № 19518

	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. Технические средства защиты информации: Учебное пособие / Титов А. А. - 2010. 194 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/653, дата обращения: 13.02.2017.
2. Торокин А.А. Инженерно-техническая защита информации: Учебное пособие для вузов. - М.: Гелиос АРВ, 2005. - 958с: табл., ил.. (наличие в библиотеке ТУСУР - 30 экз.)
3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2004. -280 с: ил.(наличие в библиотеке ТУСУР - 50 экз.)

12.2. Дополнительная литература

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации: Учебное пособие для вузов. - М.: Academia, 2006. - 330с: граф. ил. табл. (наличие в библиотеке ТУСУР - 30 экз.)
2. Технические средства защиты информации: Курс лекций / Волегов К. А., Бацула А. П., Литвинов Р. В. - 2006. 169 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/949, дата обращения: 13.02.2017.

12.3 Учебно-методические пособия

12.3.1. Литература для практических занятий

1. Исследование радиорелейных линий связи: Руководство к практическим занятиям и лабораторным работам / Максимов А. В., Филимонов А. П. - 2009. 66 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1033, дата обращения: 13.02.2017.
2. Бузов Г.А., Калинин СВ., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия-Телеком, 2005. - 414с: ил. табл.: Библиотека ТУСУР, (наличие в библиотеке ТУСУР - 60 экз.)

12.3.2 Литература для самостоятельных работ

1. Работа с портами ввода-вывода. Организация вывода информации: Методические указания к выполнению практических занятий и самостоятельной работы / Бомбизов А. А., Лощилов А. Г. - 2017. 13 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/675

12.3.3. Литература для лабораторных занятий

1. Защита речевой информации от утечки по акустическим и виброакустическим каналам: Руководство к практическим занятиям и лабораторным работам / Круглов Р. С., Южанин М. В. - 2007. 49 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/994, дата обращения: 13.02.2017.
2. Исследование проводных линий локатором-рефлектометром «БОР-1»: Руководство к практическим занятиям и лабораторным работам / Бацула А. П. - 2007. 16 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/993, дата обращения: 13.02.2017.
3. Обнаружение полупроводниковых элементов с помощью нелинейного локатора: Учебно-методическое пособие / Бацула А. П. - 2007. 21 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/988, дата обращения: 13.02.2017.
4. Инженерно-техническая защита информации: Методическое пособие по курсовому проектированию / Нелюбин А. Б., Бацула А. П. - 2007. 65 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/951, дата обращения: 13.02.2017.

Согласована на портале № 19518

5. Контроль телефонных линий и цепей электропитания на отсутствие закладных устройств: Руководство к практическим занятиям и лабораторным работам / Круглов Р. С. - 2007. 11 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/995, дата обращения: 13.02.2017.

6. Исследование устройств приема и обработки сигналов: Методические указания к лабораторным работам / Максимов А. В. — 2015. 83 с.

12.3.4. 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.

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

1. –http://edu.tusur.ru/training

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 418. Состав оборудования: Учебная мебель; Экран с электроприводом DRAPER BARONET – 1 шт.; Мультимедийный проектор TOSHIBA – 1 шт.; Компьютеры класса не ниже Intel Pentium G3220 (3.0GHz/4Mb)/4GB RAM/ 500GB с широкополосным доступом в Internet, с мониторами типа Samsung 18.5" S19C200N– 18 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft SQL-Server 2005; Matlab v6.5

13.1.2. Материально-техническое обеспечение для практических занятий

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 1 этаж, ауд. 412,416а. 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

13.1.3. Материально-техническое обеспечение для лабораторных работ

1. Контроль телефонных линий и цепей электропитания на отсутствие закладных устройств: Руководство к практическим занятиям и лабораторным работам по курсу «Технические средства защиты информации»/ Круглов Р.С. – 2007. – 11 с. – Режим доступа: – http://edu.tusur.ru/training/publications/995. 2. Защита речевой информации от утечки по акустическим и виброакустическим каналам: Руководство к практическим занятиям и лабораторным работам по курсу «Технические средства защиты информации»/ Южанин М.В., Круглов Р.С. – 2007. – 49 с. – Режим доступа: – http://edu.tusur.ru/training/publications/994. 3. Исследование проводных линий локатором-рефлектометром «БОР-1»: Руководство к

Согласована на портале № 19518

практическим занятиям и лабораторным работам по курсу «Технические средства защиты информации» / Бацула А.П. – 2007. – 16 с. – Режим доступа: – http://edu.tusur.ru/training/publications/993. 4. Обнаружение полупроводниковых элементов с помощью нелинейного локатора: Руководство к практическим занятиям и лабораторным работам по курсу «Технические средства защиты информации» / Бацула А.П. – 2007. – 21 с. – Режим доступа: – http://edu.tusur.ru/training/publications/988. 5. Инженерно-техническая защита информации: Методическое пособие по курсовому проектированию / Бацула А. П., Нелюбин А. Б. – 2007. 65 с. – Режим доступа: – http://edu.tusur.ru/training/publications/951.

13.1.4. Материально-техническое обеспечение для самостоятельной работы

Инженерно-техническая защита информации: Методическое пособие по курсовому проектированию / Бацула А. П., Нелюбин А. Б. – 2007. 65 с. – Режим доступа: – http://edu.tusur.ru/training/publications/951

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.

Журнал "Компоненты и технологии"

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.

Согласована на портале № 19518

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:

- 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 № 19518

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

Техническая защита информации

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: **4, 5**
Семестр: **8, 9**

Учебный план набора 2012 года

Разработчик:
- преподаватель каф. РЗИ А. В. Максимов

Экзамен: 8 семестр
Зачет: 9 семестр
Курсовая работа (проект): 9 семестр

Томск 2017

Согласована на портале № 19518

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-13	способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем	Должен знать технические каналы утечки информации; возможности технических разведок; способы и средства защиты информации от утечки по техническим каналам; методы и средства контроля эффективности технической защиты информации.; Должен уметь анализировать и оценивать угрозы информационной безопасности объекта.; Должен владеть методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации. ;
ПК-6	способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду	

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

Согласована на портале № 19518

2 Реализация компетенций

2.1 Компетенция ПК-13

ПК-13: способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем.

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

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	технические каналы утечки информации; • возможности технических средств перехвата информации; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; • организацию защиты информации от утечки по техническим каналам на объектах информатизации; • основы физической защиты объектов информатизации	анализировать и оценивать угрозы информационной безопасности объекта; • осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации.	методами и средствами технической защиты информации; • методами расчета и инструментального контроля показателей технической защищенности информации; • навыками безопасного использования технических средств в профессиональной деятельности.
Виды занятий	• Практические занятия; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа); • Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции;	• Практические занятия; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа); • Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции;	• Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа); • Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы;
Используемые средства оценивания	• Контрольная работа; • Отчет по индивидуальному заданию; • Отчет по	• Контрольная работа; • Отчет по индивидуальному заданию; • Отчет по	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию;

Согласована на портале № 19518

	лабораторной работе; • Опрос на занятиях; • Отчет по курсовой работе; • Отчет по практическому занятию; • Экзамен; • Зачет; • Курсовая работа (проект);	лабораторной работе; • Опрос на занятиях; • Защита курсовых проектов (работ); • Отчет по курсовой работе; • Отчет по практическому занятию; • Экзамен; • Зачет; • Курсовая работа (проект);	• Защита курсовых проектов (работ); • Отчет по курсовой работе; • Отчет по практическому занятию; • Экзамен; • Зачет; • Курсовая работа (проект);

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)	• технические каналы утечки информации; • возможности технических средств перехвата информации; ; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; ; • организацию защиты информации от утечки по техническим каналам на объектах информатизации; ; • основы физической защиты объектов информатизации ;	• технические каналы утечки информации; • возможности технических средств перехвата информации; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; • организацию защиты информации от утечки по техническим каналам на объектах информатизации; • основы физической защиты объектов информатизации • анализировать и оценивать угрозы информационной безопасности объекта; • осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации. • методами и средствами технической защиты информации; • методами расчета и инструментального контроля показателей технической	• • методами и средствами технической защиты информации; • методами расчета и инструментального контроля показателей технической защищенности информации; • навыками безопасного использования технических средств в профессиональной деятельности.;

Согласована на портале № 19518

		защищенности информации; • навыками безопасного использования технических средств в профессиональной деятельности.;	
Хорошо (базовый уровень)	• технические каналы утечки информации; • возможности технических средств перехвата информации; ; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; ; • организацию защиты информации от утечки по техническим каналам на объектах информатизации; ;	• технические каналы утечки информации; • возможности технических средств перехвата информации; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; • организацию защиты информации от утечки по техническим каналам на объектах информатизации; • основы физической защиты объектов информатизации • анализировать и оценивать угрозы информационной безопасности объекта; • осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации. • ;	• • методами и средствами технической защиты информации; • методами расчета и инструментального контроля показателей технической защищенности информации; • навыками безопасного использования технических средств в профессиональной деятельности.;
Удовлетворительно (пороговый уровень)	• технические каналы утечки информации; • возможности технических средств перехвата информации; ; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; ;	• технические каналы утечки информации; • возможности технических средств перехвата информации; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; • ;	• • методами и средствами технической защиты информации; • методами расчета и инструментального контроля показателей технической защищенности информации; • навыками безопасного использования технических средств в профессиональной деятельности.;

2.2 Компетенция ПК-6

ПК-6: способностью применять технологии обеспечения информационной безопасности

Согласована на портале № 19518

телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду.

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	• технические каналы утечки информации; • возможности технических средств перехвата информации; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; • организацию защиты информации от утечки по техническим каналам на объектах информатизации; • основы физической защиты объектов информатизации	•анализировать и оценивать угрозы информационной безопасности объекта; • осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации.	методами и средствами технической защиты информации; • методами расчета и инструментального контроля показателей технической защищенности информации; • навыками безопасного использования технических средств в профессиональной деятельности.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Контрольная работа; • Отчет по индивидуальному заданию; • Отчет по лабораторной работе; • Опрос на занятиях; • Отчет по курсовой	• Контрольная работа; • Отчет по индивидуальному заданию; • Отчет по лабораторной работе; • Опрос на занятиях; • Защита курсовых	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Защита курсовых проектов (работ); • Отчет по курсовой

Согласована на портале № 19518

	работе; • Отчет по практическому занятию; • Экзамен; • Зачет; • Курсовая работа (проект);	проектов (работ); • Отчет по курсовой работе; • Отчет по практическому занятию; • Экзамен; • Зачет; • Курсовая работа (проект);	работе; • Отчет по практическому занятию; • Экзамен; • Зачет; • Курсовая работа (проект);

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)	• • технические каналы утечки информации; • возможности технических средств перехвата информации; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; • организацию защиты информации от утечки по техническим каналам на объектах информатизации; • основы физической защиты объектов информатизации ;	• • анализировать и оценивать угрозы информационной безопасности объекта; • осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации. ;	• • методами и средствами технической защиты информации; • методами расчета и инструментального контроля показателей технической защищенности информации; • навыками безопасного использования технических средств в профессиональной деятельности. ;
Хорошо (базовый уровень)	• • технические каналы утечки информации; • возможности технических средств перехвата информации; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; • организацию защиты информации от утечки по техническим каналам на объектах информатизации; ;	• • анализировать и оценивать угрозы информационной безопасности объекта; • осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации. ;	• • методами и средствами технической защиты информации; • методами расчета и инструментального контроля показателей технической защищенности информации; • навыками безопасного использования технических средств в профессиональной деятельности. ;
Удовлетворительно (пороговый уровень)	• • технические каналы утечки информации; • возможности	• • анализировать и оценивать угрозы информационной	• • методами и средствами технической защиты

Согласована на портале № 19518

	технических средств перехвата информации; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; ;	безопасности объекта; ;	информации; • навыками безопасного использования технических средств в профессиональной деятельности. ;

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 Темы индивидуальных заданий

- Система контроля и управления доступом в помещения по биометрическим параметрам.
- Анализ методов наблюдений в ИК диапазоне.
- Анализ способов получения информации с помощью средств радиотепловой разведки и анализ методов защиты.
- Защита помещения от утечки информации по радиоканалам.
- Радиоволновое сканирование

3.2 Темы опросов на занятиях

- Источники угроз безопасности информации, защищаемой техническими средствами
- Виды угроз безопасности информации, защищаемой техническими средствами
- Демаскирующие признаки сигналов
- Методы скрытия информации

3.3 Темы контрольных работ

- Виды защищаемой информации
- Свойства информации как предмета защиты
- Источники угроз безопасности информации, защищаемой техническими средствами
- Источники и носители информации, защищаемой техническими средст-вами

3.4 Экзаменационные вопросы

- Методы подавления подслушивающих закладных устройств
- Энергетическое скрытие акустического сигнала
- Технические средства подслушивания: акустические приемники, виды микрофонов
- Методы обнаружения скрытых (запрещенных к проносу) предметов на теле человека

3.5 Вопросы для подготовки к практическим занятиям, семинарам

- Измерение ПЭМИН от различных мониторов и расчет возможности приема ПЭМИН на границе контролируемой зоны
- Анализ возможности подавления цифровых диктофонов, расчет уровня требуемой мощности.
- Определение диаграммы направленности антенного устройства нелинейного локатора
- Анализ и расчет ПЭМИН от импульсного источника питания акустической системы конференцзала

3.6 Темы лабораторных работ

- Экспериментальное исследование характеристик телефонных линий с помощью локатора-рефлектометра "ОТКЛИК-2"
- Экспериментальное исследование защищенности помещений от утечки речевой информации по виброакустическому каналу.
- Обнаружение полупроводниковых элементов с помощью нелинейного локатора «КАТРАН»

Согласована на портале № 19518

– Экспериментальное исследование защищенности помещений от утечки информации по по электромагнитному каналу, с помощью спектроанализатора и антенн электромагнитного поля

– Экспериментальное исследование защищенности помещений от утечки информации по по электромагнитному каналу, с помощью сканирующего приемника электромагнитного поля и управляющей программы "ФИЛИН"

– Комплексное исследование защищенности помещений от утечек речевой информации по всем каналам с помощью набора "Пиранья".

3.7 Зачёт

– Источники угроз безопасности информации, защищаемой техническими средствами
– Виды угроз безопасности информации, защищаемой техническими средствами
– Демаскирующие признаки сигналов
– Методы скрытия информации

3.8 Темы курсовых проектов (работ)

– Теоретические аспекты методов контроля периметра
– Теоретические предпосылки разработки СВЧ подавителя радиозакладок и диктофонов.
– Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в радиорелейных системах связи, с цифровыми видами модуляции(QPSK,КАМ16-256)
– Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах связи с WI-Fi
– Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах широкополосного доступа,WIMAX
– Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах связи с ISDN
– Анализ методов несанкционированного съема информации и защиты от несанкционированного съема в системах связи с ADSL

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 формирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Технические средства защиты информации: Учебное пособие / Титов А. А. - 2010. 194 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/653, свободный.

2. Торокин А.А. Инженерно-техническая защита информации: Учебное пособие для вузов. - М.: Гелиос АРВ, 2005. - 958с: табл., ил. (наличие в библиотеке ТУСУР - 30 экз.)

3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2004. -280 с: ил. . (наличие в библиотеке ТУСУР - 50 экз.)

4.2. Дополнительная литература

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации: Учебное пособие для вузов. - М.: Academia, 2006. - 330с: граф., ил., табл. (наличие в библиотеке ТУСУР - 30 экз.)

2. Технические средства защиты информации: Курс лекций / Волегов К. А., Бацула А. П., Литвинов Р. В. - 2006. 169 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/949, свободный.

4.3. Обязательные учебно-методические пособия

4.3.1. Литература для практических занятий

Согласована на портале № 19518

1. Исследование радиорелейных линий связи: Руководство к практическим занятиям лабораторным работам / Максимов А. В., Филимонов А. П. - 2009. 66 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1033, дата обращения: 13.02.2017.

Бузов Г.А., Калинин СВ., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия-Телеком, 2005. - 414с: ил., табл.: Библиотека ТУСУР, (наличие в библиотеке ТУСУР - 60 экз.)

4.3.2. Литература для самостоятельных работ

1. Работа с портами ввода-вывода. Организация вывода информации: Методические указания к выполнению практических занятий и самостоятельной работы / Бомбизов А. А., Лощилов А. Г. - 2017. 13 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/6758

4.3.3. Литература для лабораторных занятий

1. Защита речевой информации от утечки по акустическим и виброакустическим каналам: Руководство к практическим занятиям и лабораторным работам / Круглов Р. С., Южанин М. В. - 2007. 49 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/994, дата обращения: 13.02.2017.

2. Исследование проводных линий локатором-рефлектометром «БОР-1»: Руководство к практическим занятиям и лабораторным работам / Бацула А. П. - 2007. 16 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/993, дата обращения: 13.02.2017.

3. Обнаружение полупроводниковых элементов с помощью нелинейного локатора: Учебно-методическое пособие / Бацула А. П. - 2007. 21 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/988, дата обращения: 13.02.2017.

4. Инженерно-техническая защита информации: Методическое пособие по курсовому проектированию / Нелюбин А. Б., Бацула А. П. - 2007. 65 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/951, дата обращения: 13.02.2017.

5. Контроль телефонных линий и цепей электропитания на отсутствие закладных устройств: Руководство к практическим занятиям и лабораторным работам / Круглов Р. С. - 2007. 11 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/995, дата обращения: 13.02.2017.

6.. Исследование устройств приема и обработки сигналов: Методические указания к лабораторным работам / Максимов А. В. — 2015. 83 с.

4.4. Базы данных, информационно справочные и поисковые системы

1. –http://edu.tusur.ru/training

Согласована на портале № 19518