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

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Техническая защита информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **38.05.01 Экономическая безопасность**
Направленность (профиль): **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7, 8**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	8 семестр	Всего	Единицы
1	Лекции	4	2	6	часов
2	Лабораторные работы	4	4	8	часов
3	Всего аудиторных занятий	8	6	14	часов
4	Из них в интерактивной форме	2	2	4	часов
5	Самостоятельная работа	28	62	90	часов
6	Всего (без экзамена)	36	68	104	часов
7	Подготовка и сдача зачета		4	4	часов
8	Общая трудоемкость	36	72	108	часов
		3.0		3.0	З.Е

Контрольные работы: 8 семестр - 1
Зачет: 8 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 6 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) 38.05.01 Экономическая безопасность, утвержденного 16 января 2017 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

Старший преподаватель каф.
КИБЭВС _____ Г. А. Праскурин

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

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

Декан ЗиВФ _____ И. В. Осипов

Заведующий выпускающей каф.
КИБЭВС _____ А. А. Шелупанов

Эксперт:

Доцент кафедра КИБЭВС, ТУСУР _____ А. А. Конев

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях.

1.2. Задачи дисциплины

– Задачи дисциплины – дать основы: выявление на объекте информатизации или в выделенном помещении технических каналов утчки информации; оценка уровня шумов/информативных сигналов/помех; оценка соответствия объекта информатизации или выделенного помещения требованиям по безопасности от утечки информации по техническим каналам

2. Место дисциплины в структуре ОПОП

Дисциплина «Техническая защита информации» (Б1.В.ДВ.3.2) относится к блоку 1 (вариативная часть).

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

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;

В результате изучения дисциплины студент должен:

– **знать** технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.

– **уметь** анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. пользоваться нормативными документами по защите информации.

– **владеть** методами и средствами выявления угроз безопасности автоматизированным системам; 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 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		7 семестр	8 семестр
Аудиторные занятия (всего)	14	8	6
Лекции	6	4	2
Лабораторные работы	8	4	4
Из них в интерактивной форме	4	2	2
Самостоятельная работа (всего)	90	28	62
Оформление отчетов по лабораторным работам	2	2	
Проработка лекционного материала	22	22	
Подготовка к практическим занятиям, семинарам	46	4	42

Выполнение контрольных работ	20		20
Всего (без экзамена)	104	36	68
Подготовка и сдача зачета	4		4
Общая трудоемкость ч	108	36	72
Зачетные Единицы	3.0	3.0	

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	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
7 семестр					
1 Концепция инженерно-технической защиты информации	1	0	4	5	ОК-12
2 Теоретические основы инженерно-технической защиты информации	1	0	4	5	ОК-12
3 Физические основы защиты информации	1	0	8	9	ОК-12
4 Технические средства добывания и инженерно-технической защиты информации	1	4	4	9	ОК-12
5 Организационные основы инженерно-технической защиты информации	0	0	4	4	ОК-12
6 Методическое обеспечение инженерно-технической защиты информации	0	0	4	4	ОК-12
Итого за семестр	4	4	28	36	
8 семестр					
7 Организационные основы инженерно-технической защиты информации	1	2	20	23	ОК-12
8 Методическое обеспечение инженерно-технической защиты информации	1	2	42	45	ОК-12
Итого за семестр	2	4	62	68	
Итого	6	8	90	104	

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Концепция инженерно-технической защиты информации	Характеристика инженерно-технической защиты информации. Технические средства и методы защиты информации. Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели эффективности инженерно-технической защиты информации.Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Основные направления инженерно-технической защиты информации. Принципы защиты информации техническими средствами.	1	ОК-12
	Итого	1	
2 Теоретические основы инженерно-технической защиты информации	Информация как предмет защиты. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Понятие о текущей и эталонной признаковой структуре.Источники опасных сигналов. Понятие об опасном сигнале. Опасные сигналы и их источники. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и характеристика основных и вспомогательных технических средств и систем. Побочные электромагнитные излучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Классификация технической разведки по видам носителя информации	1	ОК-12

	и средств разведки. Возможности видов технической разведки. Основные направления развития технической разведки. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их возможности.		
	Итого	1	
3 Физические основы защиты информации	Распространение сигналов в технических каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах.Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигналов различных технических каналов утечки информации.Физические процессы подавление опасных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.	1	ОК-12
	Итого	1	
4 Технические средства добывания и инженерно-технической защиты информации	Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в	1	ОК-12

	оптическом и радиодиапазонах. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов. Средства звукоизоляции из звукопоглощения. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Генераторы линейного и пространственного зашумления.		
	Итого	1	
Итого за семестр		4	
8 семестр			
7 Организационные основы инженерно-технической защиты информации	Государственная система защиты информации. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам. Методы расчета и инструментального контроля показателей защиты информации. Особенности инструментального контроля эффективности инженерно-технической защиты информации.	1	ОК-12
	Итого	1	
8 Методическое обеспечение инженерно-технической защиты информации	Моделирование инженерно-технической защиты информации. Концепция и методы инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Ме-	1	ОК-12

	тодические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.Принципы оценки эффективности инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в защищаемых помещениях. Принципы оценки размеров опасных зон I и II.		
	Итого	1	
Итого за семестр		2	
Итого		6	

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
Предшествующие дисциплины								
1 Основы информационной безопасности	+	+			+	+		

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

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

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

Компетенции	Виды занятий			Формы контроля
	Лекции	Лабораторные работы	Самостоятельная работа	
ОК-12	+	+	+	Контрольная работа, Экзамен, Отчет по лабораторной работе, Опрос на занятиях, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в та-

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

Методы	Интерактивные лекции	Интерактивные лабораторные занятия	Всего
7 семестр			
Мини-лекция	1		1
IT-методы	1		1
Презентации с использованием видеофильмов с обсуждением			0
Итого за семестр:	2	0	2
8 семестр			
Работа в команде		1	1
Решение ситуационных задач		1	1
Итого за семестр:	0	2	2
Итого	2	2	4

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
7 семестр			
4 Технические средства добывания и инженерно-технической защиты информации	Статистический анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещении.	1	ОК-12
	Нелинейная локация.	1	
	Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля.	1	
	Аппаратно-программный комплекс имитации сигналов закладочных устройств «АВРОРА-Т».	1	
	Итого	4	
Итого за семестр		4	
8 семестр			
7 Организационные основы инженерно-технической защиты информации	Охрана выделенных помещений. Пожарная сигнализация.	1	ОК-12
	Охрана выделенных помещений. Охранная сигнализация.	1	

	Итого	2	
8 Методическое обеспечение инженерно-технической защиты информации	Ограничение доступа в выделенное помещение. Система контроля и управления доступом.	1	ОК-12
	Охрана выделенных помещений. Система видеонаблюдения.	1	
	Итого	2	
Итого за семестр		4	
Итого		8	

8. Практические занятия (семинары)

Не предусмотрено РУП

9. Самостоятельная работа

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

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
7 семестр				
1 Концепция инженерно-технической защиты информации	Проработка лекционного материала	4	ОК-12	Опрос на занятиях
	Итого	4		
2 Теоретические основы инженерно-технической защиты информации	Проработка лекционного материала	4	ОК-12	Опрос на занятиях, Экзамен
	Итого	4		
3 Физические основы защиты информации	Подготовка к практическим занятиям, семинарам	4	ОК-12	Опрос на занятиях, Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	4		
	Итого	8		
4 Технические средства добывания и инженерно-технической защиты информации	Проработка лекционного материала	2	ОК-12	Опрос на занятиях, Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
5 Организационные основы инженерно-технической защиты информации	Проработка лекционного материала	4	ОК-12	Опрос на занятиях, Экзамен
	Итого	4		
6 Методическое обеспечение инженерно-технической защиты	Проработка лекционного материала	4	ОК-12	Опрос на занятиях, Экзамен
	Итого	4		

информации				
Итого за семестр		28		
8 семестр				
7 Организационные основы инженерно-технической защиты информации	Подготовка к практическим занятиям, семинарам	20	ОК-12	Отчет по практическому занятию, Экзамен
	Итого	20		
8 Методическое обеспечение инженерно-технической защиты информации	Выполнение контрольных работ	20	ОК-12	Контрольная работа, Отчет по практическому занятию, Экзамен
	Подготовка к практическим занятиям, семинарам	22		
	Итого	42		
Итого за семестр		62		
	Подготовка и сдача зачета	4		Зачет
Итого		94		

9.1. Темы контрольных работ

1. Информация как объект защиты
2. Технические каналы утечки информации
3. Характеристики акустического и виброакустического каналов утечки информации
4. Характеристики канала ПЭМИН
5. Методика измерений акустических сигналов
6. Методика измерения сигналов ПЭМИН
7. Методика защиты от утечки по акустическом каналу
8. Методика защиты от утечки по каналу ПЭМИН

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

Не предусмотрено

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=176315&rnd=244973.2538529920&from=121414-0#0

2. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200126&rnd=244973.246476619&from=165971-0#0

3. Закон Российской Федерации «О персональных данных» от 27 июля 2006 г. №152-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200556&rnd=244973.626813432&from=166051-0#0

4. Торокин А. А. Инженерно-техническая защита информации. М: «Гелиос АРВ», 2005 г. 960 с. (наличие в библиотеке ТУСУР - 30 экз.)

12.2. Дополнительная литература

1. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 1 / Министерство образова-

ния и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 150[2] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)

2. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 2 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 185[1] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)

3. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 3 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 98[2] с. : ил., табл. (наличие в библиотеке ТУСУР - 81 экз.)

4. Радиоэлектронная разведка и радиомаскировка : / В. П. Демин, А. И. Куприянов, А. В. Сахаров. - М. : МАИ, 1997. - 155, [1] с. : ил., табл. (наличие в библиотеке ТУСУР - 1 экз.)

5. Защита и охрана личности, собственности, информации : Справочное пособие / Алексей Васильевич Петраков. - М. : Радио и связь, 1997. - 320 с. : ил. (наличие в библиотеке ТУСУР - 11 экз.)

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1017, дата обращения: 06.06.2017.

2. Защита информации: Методические указания к выполнению лабораторных работ / Спицын В. Г. - 2012. 77 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1826, дата обращения: 06.06.2017.

3. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2261, дата обращения: 06.06.2017.

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.

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

1. http://portal.tusur.ru; http://www.lib.tusur.ru – образовательный портал университета;
2. http://www.iqlib.ri – электронная интернет-библиотека;
3. http://www.biblioclub.ru – полнотестовая электронная библиотека;
4. http://www.elibrary.ru – научная электронная библиотека;
5. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.

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 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 лабораторных работ

Интерактивная доска с лицензионным программным обеспечением и мультимедиа-проектор Лаборатория технической защиты информации Лаборатория технических средств охраны

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Ce1егоп D336 2.8ГГц. - 7 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.

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	Собеседование по вопросам к зачету,	Преимущественно устная проверка

зрения	опрос по терминам	(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.

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): **38.05.01 Экономическая безопасность**
Направленность (профиль): **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7, 8**

Учебный план набора 2013 года

Разработчик:
- Старший преподаватель каф. КИБЭВС Г. А. Праскурин

Зачет: 8 семестр

Томск 2017

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
ОК-12	способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Должен знать технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.; Должен уметь анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. пользоваться нормативными документами по защите информации. ; Должен владеть методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации. ;

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	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми	Работает при прямом наблюдении

уровень)		для выполнения простых задач	

2 Реализация компетенций

2.1 Компетенция ОК-12

ОК-12: способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.

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 разведок, способы и средства защиты информации от утечки по техническим каналам.	анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.	методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.
Виды занятий	• Интерактивные лабораторные занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные лекции;	• Интерактивные лабораторные занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные лекции;	• Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Экзамен; • Отчет по лабораторной работе; • Опрос на занятиях; • Отчет по практическому занятию; • Зачет;	• Контрольная работа; • Экзамен; • Отчет по лабораторной работе; • Опрос на занятиях; • Отчет по практическому занятию; • Зачет;	• Отчет по лабораторной работе; • Экзамен; • Отчет по практическому занятию; • Зачет;

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)	• Физические основы, количественные и качественные характеристики технических каналов утески информации, методы оценки эффек-	• Умеет анализировать и оценивать угрозы информационной безопасности объекта от различных источников. Применяет отечествен-	• Свободно владет разными методами и средствами выявления угроз безопасности автоматизированным системам. Свободно вла-

	тивности технических разведок, методы оценки эффективности защиты информации от утечки по техническим каналам.;	ные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем с повышеными требования по безопасности нформации;	дет несколькими методами технической защиты информации. Свободно использует методы расчета и инструментального контроля показателей технической защиты информации;
Хорошо (базовый уровень)	• Знает характеристики технических каналов утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.;	• Применяет базовые методы анализа и оценки угрозы информационной безопасности объекта. Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.;	• Может применять и обосновывать методы и средствами выявления угроз безопасности автоматизированным системам, методы технической защиты информации, методы расчета и инструментального контроля показателей технической защиты информации.;
Удовлетворительно (пороговый уровень)	• Дает определения основных понятий технических каналов утечки информации, технических разведок.;	• Умеет работать со справочной литературой. Решает типовые задачи;	• Может применять некоторые методы и средства выявления угроз безопасности автоматизированным системам, методы технической защиты информации.;

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 Зачёт

– 1. Дайте определение информации, документированной информации. Каково отличие государственной тайны, конфиденциальной информации и открытой информации. 2. Классификация технической разведки. Эффективность добывания информации технической разведкой. 3. Государственная система защиты информации. Эффективность защиты информации. 4. Основные объекты защиты информации. 5. Дайте определение демаскирующих признаков. Для чего они используются. Приведите примеры. 6. Дайте определение терминам Контролируемая зона, Опасная зона, Опасная зона 1, Опасная зона 2. 7. Состав технического канала утечки информации. 8. Классификация технических каналов утечки информации. 9. Перечислите технические каналы утечки информации, обрабатываемой ОТСС. Приведите примеры. 10. Перечислите технические каналы утечки информации при передаче по каналам связи. Приведите примеры. 11. Перечислите каналы утечки речевой информации. Приведите примеры. 12. Перечислите каналы утечки видовой информации. Приведите примеры. 13. Каково влияние паразитных емкостных, индуктивных и резистивных связей в каналах связи. 14. Перечислите методы противодействия утечке информации по техническим каналам.

3.2 Темы опросов на занятиях

– Характеристика инженерно-технической защиты информации. Технические средства и

методы защиты информации. Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели эффективности инженерно-технической защиты информации.

– Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Основные направления инженерно-технической защиты информации. Принципы защиты информации техническими средствами.

– Информация как предмет защиты. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Понятие о текущей и эталонной признаковой структуре.

– Источники опасных сигналов. Понятие об опасном сигнале. Опасные сигналы и их источники. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и характеристика основных и вспомогательных технических средств и систем. Побочные электромагнитные излучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации.

– Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки. Основные направления развития технической разведки.

– Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их возможности.

– Распространение сигналов в технических каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах.

– Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигналов различных технических каналов утечки информации.

– Физические процессы подавление опасных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.

– Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.

– Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов. Средства звукоизоляции из звукопоглощения. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Генераторы линейного и пространственного зашумления.

– Государственная система защиты информации. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.

– Контроль эффективности инженерно-технической защиты информации. Виды контроля

эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам. Методы расчета и инструментального контроля показателей защиты информации. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

– Моделирование инженерно-технической защиты информации. Концепция и методы инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.

– Принципы оценки эффективности инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в защищаемых помещениях. Принципы оценки размеров опасных зон I и II.

3.3 Темы контрольных работ

– Информация как объект защиты
– Технические каналы утечки информации
– Характеристики акустического и виброакустического каналов утечки информации
– Характеристики канала ПЭМИН
– Методика измерений акустических сигналов
– Методика измерения сигналов ПЭМИН
– Методика защиты от утечки по акустическом каналу
– Методика защиты от утечки по каналу ПЭМИН

3.4 Экзаменационные вопросы

– 15. Способы скрытого видеонаблюдения. Характеристики оборудования для скрытого видеонаблюдения.

– 16. Способы скрытого прослушивания переговоров в помещении. Демаскирующие признаки радиозакладок. Демаскирующие признаки проводных закладок.

– 17. Способы прослушивания переговоров по телефонным линиям. Демаскирующие признаки акустических закладок типа «телефонное ухо».

– 18. Направленные микрофоны. Принцип действия.

– 19. Охранные системы. Назначение. Структура. Приведите примеры охранных систем объектов и помещений.

– 20. Датчики охранных систем. Принципы действия датчиков.

– 21. Охранное видеонаблюдение. Назначение. Структура. Основные характеристики.

– 22. Средства радиотехнической разведки. Состав. Характеристики.

– 23. Охрана объектов. Особенности охраны объектов различного класса. Задачи средств охраны объектов.

– 24. Периметровые средства охраны. Датчики периметровых систем охраны.

– 25. Охрана выделенных (защищаемых) помещений. Технические средства охраны помещений.

– 26. Экранирование электромагнитных волн.

– 27. Экранирование акустических сигналов.

– 28. Фильтрация опасных сигналов. Приведите примеры.

– 29. Маскировка опасных сигналов зашумлением. Приведите примеры.

– 30. Металлодетекторы. Сферы применения. Принцип действия.

– 31. Локаторы нелинейностей. Сферы применения. Принцип действия.

– 32. Аттестация объектов информатизации по требованиям безопасности. Назначение. Порядок проведения аттестации.

– 33. Специальная проверка. Специальное обследование. Специальное исследование.

– 34. Проведение измерений акустических и виброакустических характеристик. Приведите примеры.

– 35. Проведение измерений побочных электромагнитных излучений. Приведите примеры.

3.5 Вопросы для подготовки к практическим занятиям, семинарам

– Какими техническими средстчами проводится анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещении.

– Принципы и назначение нелинейная локация.

– Методика обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля.

– Технологии охраны выделенных помещений. Датчики пожарной сигнализации. Датчики охранной сигнализации.

– Технологии контроля и ограничения доступа в выделенное помещение. Система контроля и управления доступом.

– Организация систем видеонаблюдения.

3.6 Темы лабораторных работ

– Статистический анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещении.

– Нелинейная локация.

– Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля.

– Аппаратно-программный комплекс имитации сигналов закладочных устройств «АВРОРА-Т».

– Охрана выделенных помещений. Пожарная сигнализация.

– Охрана выделенных помещений. Охранная сигнализация.

– Ограничение доступа в выделенное помещение. Система контроля и управления доступом.

– Охрана выделенных помещений. Система видеонаблюдения.

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. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=176315&rnd=244973.2538529920&from=121414-0#0

2. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200126&rnd=244973.246476619&from=165971-0#0

3. Закон Российской Федерации «О персональных данных» от 27 июля 2006 г. №152-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]. - http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200556&rnd=244973.626813432&from=166051-0#0

4. Торокин А. А. Инженерно-техническая защита информации. М: «Гелиос АРВ», 2005 г. 960 с. (наличие в библиотеке ТУСУР - 30 экз.)

4.2. Дополнительная литература

1. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 1 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 150[2] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)

2. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 2 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 185[1] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)

3. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 3 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 98[2] с. : ил., табл. (наличие в библиотеке ТУСУР - 81 экз.)

4. Радиоэлектронная разведка и радиомаскировка : / В. П. Демин, А. И. Куприянов, А. В. Сахаров. - М. : МАИ, 1997. - 155, [1] с. : ил., табл. (наличие в библиотеке ТУСУР - 1 экз.)

5. Защита и охрана личности, собственности, информации : Справочное пособие / Алексей Васильевич Петраков. - М. : Радио и связь, 1997. - 320 с. : ил. (наличие в библиотеке ТУСУР - 11 экз.)

4.3. Обязательные учебно-методические пособия

1. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1017, свободный.

2. Защита информации: Методические указания к выполнению лабораторных работ / Спицын В. Г. - 2012. 77 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1826, свободный.

3. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2261, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. http://portal.tusur.ru; http://www.lib.tusur.ru – образовательный портал университета;
2. http://www.iqlib.ri – электронная интернет-библиотека;
3. http://www.biblioclub.ru – полнотестовая электронная библиотека;
4. http://www.elibrary.ru – научная электронная библиотека;
5. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.