МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Техническая защита информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Специализация: **Экономико-правовое обеспечение экономической безопасности**
Направленность (профиль): **Регламентация работы персонала организации при обеспечении экономической и информационной 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	0	4	4	часов
8	Общая трудоемкость	36	72	108	часов
				3.0	З.Е.

Контрольные работы: 8 семестр - 1
Зачет: 8 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 23.08.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 36217

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 15 » 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16.01.2017 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Старший преподаватель каф. КИБЭВС _____ Г. А. Праскурин

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ЗиВФ _____ И. В. Осипов

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры КИБЭВС _____ А. А. Конев

Доцент кафедры КИБЭВС _____ К. С. Сарин

Согласована на портале № 36217

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; по вопросам соблюдения в профессиональной деятельности требований, установленных нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечения соблюдение режима секретности

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.1.2) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности.

Последующими дисциплинами являются: Преддипломная практика, Управление информационной безопасностью.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

В результате изучения дисциплины обучающийся 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

Согласована на портале № 36217

Оформление отчетов по лабораторным работам	6	6	0
Проработка лекционного материала	18	18	0
Подготовка к практическим занятиям, семинарам	46	4	42
Выполнение контрольных работ	20	0	20
Всего (без экзамена)	104	36	68
Подготовка и сдача зачета	4	0	4
Общая трудоемкость, ч	108	36	72
Зачетные Единицы	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	Лек., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр					
1 Концепция инженерно-технической защиты информации	1	0	4	5	ПК-20
2 Теоретические основы инженерно-технической защиты информации	1	0	4	5	ПК-20
3 Физические основы защиты информации	1	0	8	9	ПК-20
4 Технические средства добывания и инженерно-технической защиты информации	1	4	12	17	ПК-20
Итого за семестр	4	4	28	36	
8 семестр					
5 Организационные основы инженерно-технической защиты информации	1	2	20	23	ПК-20
6 Методическое обеспечение инженерно-технической защиты информации	1	2	42	45	ПК-20
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	Характеристика инженерно-технической	1	ПК-20

Согласована на портале № 36217

инженерно-технической защиты информации	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.		
	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 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	1	ПК-20

Согласована на портале № 36217

	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	ПК-20
	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 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	1	ПК-20

Согласована на портале № 36217

	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			
5 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	ПК-20
	Итого	1	
6 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. 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.	1	ПК-20

Согласована на портале № 36217

	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
Предшествующие дисциплины						
1 Организационное и правовое обеспечение информационной безопасности	+	+	+	+	+	+
2 Основы информационной безопасности	+	+			+	+
Последующие дисциплины						
1 Преддипломная практика	+	+	+	+	+	+
2 Управление информационной безопасностью	+	+	+	+	+	+

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

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

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

Компетенции	Виды занятий			Формы контроля
	Лек.	Лаб. раб.	Сам. раб.	
ПК-20	+	+	+	Контрольная работа, Отчет по лабораторной работе, Опрос на занятиях, Зачет, Тест

6. Интерактивные методы и формы организации обучения

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

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные лекции, ч	Интерактивные лабораторные занятия, ч	Всего, ч
7 семестр			
Мини-лекция	1		1

Согласована на портале № 36217

IT-методы	1		1
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	ПК-20
	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			
5 Организационные основы инженерно-технической защиты информации	Охрана выделенных помещений. Пожарная сигнализация.	1	ПК-20
	Охрана выделенных помещений. Охранная сигнализация.	1	
	Итого	2	
6 Методическое обеспечение инженерно-технической защиты информации	Ограничение доступа в выделенное помещение. Система контроля и управления доступом.	1	ПК-20
	Охрана выделенных помещений. Система видеонаблюдения.	1	
	Итого	2	
Итого за семестр		4	
Итого		8	

8. Практические занятия (семинары)

Не предусмотрено РУП.

9. Самостоятельная работа

Согласована на портале № 36217

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	ПК-20	Зачет, Опрос на занятиях, Тест
	Итого	4		
2 Теоретические основы инженерно-технической защиты информации	Проработка лекционного материала	4	ПК-20	Зачет, Опрос на занятиях, Тест
	Итого	4		
3 Физические основы защиты информации	Подготовка к практическим занятиям, семинарам	4	ПК-20	Зачет, Опрос на занятиях, Тест
	Проработка лекционного материала	4		
	Итого	8		
4 Технические средства добывания и инженерно-технической защиты информации	Проработка лекционного материала	6	ПК-20	Зачет, Опрос на занятиях, Тест
	Оформление отчетов по лабораторным работам	6		
	Итого	12		
Итого за семестр		28		
8 семестр				
5 Организационные основы инженерно-технической защиты информации	Подготовка к практическим занятиям, семинарам	20	ПК-20	Зачет, Опрос на занятиях, Тест
	Итого	20		
6 Методическое обеспечение инженерно-технической защиты информации	Выполнение контрольных работ	20	ПК-20	Зачет, Контрольная работа, Тест
	Подготовка к практическим занятиям, семинарам	22		
	Итого	42		
Итого за семестр		62		
	Подготовка и сдача зачета	4		Зачет

Согласована на портале № 36217

Итого	94		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Инженерно-техническая защита информации [Электронный ресурс]: Учебное пособие / Титов А. А. - 2010. 195 с. — Режим доступа: https://edu.tusur.ru/publications/654 (дата обращения: 19.05.2018).

2. Защита информации от утечки по техническим каналам [Электронный ресурс]: Учебное пособие / Голиков А. М. - 2015. 256 с. — Режим доступа: https://edu.tusur.ru/publications/5263 (дата обращения: 19.05.2018).

3. Технические средства охраны [Электронный ресурс]: Учебное пособие / Дементьев А. Н., Дементьева Г. В. - 2012. 119 с. — Режим доступа: https://edu.tusur.ru/publications/2352 (дата обращения: 19.05.2018).

12.2. Дополнительная литература

1. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220985&rnd=47EEB9B8FFC90E642EB42D004D5872CA&from=176315-0#06808284158820568 (дата обращения: 19.05.2018).

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]: — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&n=286904&base=LAW&rnd=47EEB9B8FFC90E642EB42D004D5872CA&from=296555-6#029432728300970434 (дата обращения: 19.05.2018).

3. Закон Российской Федерации «О персональных данных» от 27 июля 2006 г. №152-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&n=286959&base=LAW&rnd=47EEB9B8FFC90E642EB42D004D5872CA&from=221444-6#07686238316330771 (дата обращения: 19.05.2018).

4. Зайцев, Александр Петрович. Технические средства обеспечения информационной безопасности [] : Учебное пособие для вузов. Ч. 2 : Средства защиты информации по техническим каналам : учебное пособие. - Томск : ТМЦДО , 2004. - 279 с. (наличие в библиотеке ТУСУР - 30 экз.)

5. Зайцев, Александр Петрович. Технические средства обеспечения информационной безопасности [] : Учебное пособие для вузов. Ч. 1 : Технические каналы утечки информации. - Томск : ТМЦДО , 2004. - 199 с. (наличие в библиотеке ТУСУР - 30 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Зайцев, Александр Петрович. Технические средства и методы защиты информации : Лабораторный практикум: Учебное пособие. - Томск : В-Спектр , 2007. - 119[1] с. (наличие в библиотеке ТУСУР - 65 экз.)

2. Защита информации [Электронный ресурс]: Методические указания к выполнению лабораторных работ / Спицын В. Г. - 2012. 77 с. — Режим доступа: https://edu.tusur.ru/publications/1826 (дата обращения: 19.05.2018).

3. Защита информации [Электронный ресурс]: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. — Режим доступа: https://edu.tusur.ru/publications/2261 (дата обращения: 19.05.2018).

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

Согласована на портале № 36217

обращения: 19.05.2018).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. https://edu.tusur.ru – образовательный портал университета;
2. http://www.iqlib.ru – 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 и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория технической защиты информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 512 ауд.

Описание имеющегося оборудования:

- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Нелинейный локатор NR 900 EM;
- Индикатор поля ST06 SEL SP-77 "Ловец";
- Многофунцкциональный поисковый прибор ST 034;
- Анализатор спектра цифровой GSP-7930;
- Ручной металлодетектор «АКА»;
- Программно-аппаратный комплекс для проведения акустических и виброакустических измерений СПРУТ 7;
- Программно-аппаратный измерительный комплекс «Гриф АЭ-1001»;
- Система защиты от утечки информации Гром ЗИ-4Б;
- Блокиратор сотовых телефонов C-GUARD 300YK;
- Система виброакустической защиты "Соната-АВ" мод. 1М;

Согласована на портале № 36217

- Пьезоизлучатель ПИ-45; Аудиоизлучатель АИ-65;
- Электронно-оптическое устройство "Алмаз";
- Электронно-оптическое устройство "Вега";
- Портативная установка НОРКА-МАКСИ-Д;
- Детектор радиополя D-008;
- RS turboMobile – L;
- Программно-аппаратный компьютеризированный комплекс «Легенда»;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- Kaspersky endpoint security
- Microsoft Windows 10

Лаборатория защищенных автоматизированных систем

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 511 ауд.

Описание имеющегося оборудования:

- Компьютеры класса не ниже AMD A6-3670 / Asus F1A75-M Pro / DDR3 4 Gb/ ST3250410AS 250 Gb, (5 шт.);
- Сетевой контроллер СКУД Gate-4000 UPS;
- Стенд монтажный стол;
- Контроллер управления доступом UnitECO LOCK 2S-LO-SMB;
- Турникет PERCo-KT03/600-1;
- Охранное устройство Мираж-GSM-A4-03;
- ИК извещатель, «стандарт» РАПИД;
- Извещатель радиоволновый Астра-552;
- Комбинированный извещатель Астра-8;
- Приемопередатчики видеосигнала по витой паре на TTP111VLH; видеосервер Domination D7-8-H264;
- Видеорегистратор Videorox DVR VR 3294;
- Стандартная цветная видеокамера под объектив MSC-512S;
- Купольная видеокамера SCW-422;
- Пульт управления камерами SPEED DOME SCJ-200;
- Видео камера сетевая SPEED DOME Beward BD75-5;
- Уличная видеокамера SPEED;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- Kaspersky endpoint security
- Microsoft Windows 10

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную

Согласована на портале № 36217

информационно-образовательную среду университета.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

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

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Какой канал утечки информации использует эффект высокочастотного облучения для перехвата информации обрабатываемой в технических средствах?

1) Акустоэлектрический
2) Параметрический
3) Электрический
4) Электромагнитный

2. При передачи информации по каналам связи, какой канал утечки информации возникает в результате возникновения вокруг высокочастотного кабеля электромагнитного поля?

1) Электромагнитный канал
2) Индукционный канал
3) Паразитные связи
4) Электрический канал

3. Каким из каналов утечки речевой информации является окно?

1) Акустическим
2) Виброакустическим
3) Оптическим
4) Все варианты

4. Как называется устройство про помощи которого выполняется измерение ограждающих конструкций при проведении виброакустических измерений разборчивости речи?

1) Акселерометр

Согласована на портале № 36217

2) Микрофон
3) Акустический излучатель
4) Лучевая трубка

5. Какой канал утечки информации возникает за счет преобразований акустических сигналов в электрические различными радиоэлектронными устройствами, обладающими «микрофонным эффектом», а также путем «высокочастотного навязывания»

1) Акустоэлектрический канал
2) Оптико-электронный канал
3) Гидроакустичекий канал
4) Вибрационный канал

6. Устройство, используемое для проведения измерений ТС на побочные электромагнитные излучения (ПЭМИ)?

1) Анализатор спектра
2) Шумомер
3) Низкочастотный анализатор
4) Все варианты

7. Устройства, подлежащие исследованию на побочные электромагнитные излучения и наводки (ПЭМИН)?

1) Накопители на жестких дисках
2) Принтер
3) Клавиатура
4) Все варианты

8. Каким каналом утечки речевой информации являются системы отопления в помещении?

1) Акустический
2) Видовой
3) Виброакустический
4) Все варианты

9. Каким каналом утечки речевой информации является дверь в выделенное помещение?

1) Параметрический
2) Видовой
3) Акустический
4) Оптико-электронный

10. Что из нижеперечисленного НЕ относится к акустическому каналу утечки речевой информации?

1) Окно
2) Дверь
3) Батареи и трубы отопления
4) Все варианты

11. Какая из среднегеометрических частот не входит в стандартные октавные полосы?

1) 250 Гц
2) 1 кГц
3) 500 Гц
4) 750 Гц

12. Создаваемый уровень звукового давления при выступлении человека в аудитории без средств звукоусиления?

1) 100 дБ
2) 70 дБ
3) 84 дБ
4) 50 дБ

13. Создаваемый уровень звукового давления при выступлении человека в аудитории со средствами звукоусиления?

1) 100 дБ
2) 70 дБ
3) 84 дБ

Согласована на портале № 36217

4) 50 дБ

14. При превышении какого значения разборчивости речи можно говорить о достижении уровня непреднамеренного прослушивания?

1) 10%
2) 20%
3) 30%
4) 40%

15. При превышении какого значения разборчивости речи можно говорить о достижении уровня сокрытия факта переговоров?

1) 10%
2) 20%
3) 30%
4) 40%

16. При проведении акустических измерений разборчивости речи через ограждающие конструкции на каком расстоянии от пола должен располагаться излучатель тестового акустического сигнала?

1) 0.5м
2) 1.7м
3) 1м
4) 1.5м

17. При проведении акустических измерений разборчивости речи через ограждающие конструкции на каком расстоянии от ограждающей конструкции должен располагаться микрофон?

1) 1.5м
2) 0.7м
3) 0.5м
4) 1м

18. При проведении измерений системы отопления, представляющей собой виброакустический канал утечки речевой информации на каком расстоянии от места выхода трубы из выделенного помещения должен закрепляться акселерометр?

1) 50см
2) 15см
3) 70см
4) 30см

19. При помощи какого устройства выполняется измерение ограждающих конструкций при проведении виброакустических измерений разборчивости речи?

1) Акустический излучатель
2) Акселерометр
3) Микрофон
4) Лучевая трубка

20. Что изучается при определение значений сигналов АЭП речевого диапазона частот в отходящей от ВТСС линии, выходящей за пределы КЗ?

1) Телефония
2) Система сигнализации
3) Цепи электропитания
4) Все перечисленное

14.1.2. 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.

Согласована на портале № 36217

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

Согласована на портале № 36217

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.

14.1.3. 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.

14.1.4. Темы контрольных работ

Целии задачи защиты информации.

Основные направления инженерно-технической защиты информации.

Принципы защиты информации техническими средствами.

Технические каналы утечки информации. Их характеристики.

Источники опасных сигналов

Методы инженерной защиты и технической охраны объектов.

Защита речевой информации от утечки по акустическому и виброакустическому каналам.

Защита информации от утечки по каналу побочных электромагнитных излучений.

Выявление устройств негласного сбора и нформации и закладных устройств.

Государственная система защиты информации. Лицензирование деятельности по защите информации. Сертификация средств защиты информации. Аттестация объектов информатизации по требованиям безопасности информации.

14.1.5. 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.

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Согласована на портале № 36217

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 36217