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

Защита информации в системах беспроводной связи

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль): **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **4**
Семестр: **8**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Из них в интерактивной форме	16	16	часов
5	Самостоятельная работа	54	54	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е

Экзамен: 8 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «16» 6 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16 ноября 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

инженер каф. БИС	_____	А. Ю. Исхаков
доцент каф. БИС	_____	О. О. Евсютин

Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

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

Декан ФБ	_____	Е. М. Давыдова
Заведующий выпускающей каф. БИС	_____	Р. В. Мещеряков

Эксперт:

старший преподаватель каф. КИБЭВС	_____	Г. А. Праскурин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Обучить студентов основам построения и эксплуатации распределенных автоматизированных систем, использующих беспроводные каналы передачи данных, принципам и методам защиты информации в подобных системах, навыкам комплексного проектирования, построения и анализа защищенных систем беспроводной связи

1.2. Задачи дисциплины

- – изучение технологий и протоколов беспроводной передачи данных;
- – рассмотрение архитектуры и классификации распределенных систем беспроводной связи;
- – выделение основных угроз информации в системах беспроводной связи;
- – изучение программно-аппаратных средств обеспечения безопасности в системах беспроводной связи.
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации в системах беспроводной связи» (Б1.Б.38.3) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Администрирование сетей ЭВМ, Моделирование систем и сетей телекоммуникаций.

Последующими дисциплинами являются: Измерения в телекоммуникационных системах, Информационная безопасность телекоммуникационных систем, Проектирование защищенных телекоммуникационных систем.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПСК-10.4 способностью применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации;
- ПСК-10.3 способностью оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации;
- ПСК-10.2 способностью формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем;

В результате изучения дисциплины студент должен:

- **знать** технологии беспроводной передачи данных; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.
- **уметь** применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в беспроводных сетях передачи данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов.
- **владеть** навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений.

4. Объем дисциплины и виды учебной работы

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

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		8 семестр
Аудиторные занятия (всего)	54	54
Лекции	18	18
Лабораторные работы	36	36
Из них в интерактивной форме	16	16
Самостоятельная работа (всего)	54	54
Оформление отчетов по лабораторным работам	32	32
Проработка лекционного материала	18	18
Написание рефератов	4	4
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость ч	144	144
Зачетные Единицы	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Основы и особенности беспроводных технологий	2	0	8	10	ПСК-10.2, ПСК-10.3
2 Принципы передачи информации в радиоэфире	4	6	3	13	ПСК-10.2, ПСК-10.3, ПСК-10.4
3 Виды беспроводных сетей. Основные угрозы информационной безопасности	4	18	23	45	ПСК-10.2, ПСК-10.3, ПСК-10.4
4 Построение защищенных распределенных систем на основе беспроводных сетей	4	6	13	23	ПСК-10.2, ПСК-10.3, ПСК-10.4
5 Методика испытаний систем беспроводной связи	4	6	7	17	ПСК-10.2, ПСК-10.3
Итого за семестр	18	36	54	108	
Итого	18	36	54	108	

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Основы и особенности беспроводных технологий	История развития беспроводной связи. Отличия проводных и беспроводных технологий передачи данных.Классификация беспроводных технологий по дальности действия, по топологии, по области действия.	2	ПСК-10.3
	Итого	2	
2 Принципы передачи информации в радиоэфире	Пакетная и синхронная передача в радиоэфире. Методы модуляции и технологии передачи. Методы доступа к среде. Методы широкополосной передачи сигнала.	4	ПСК-10.3, ПСК-10.4
	Итого	4	
3 Виды беспроводных сетей. Основные угрозы информационной безопасности	Классификация беспроводных сетей-.Подслушивание.Отказ в обслуживании.Глушение клиентской станции.Глушение базовой станции.Угрозы криптозащиты	4	ПСК-10.2, ПСК-10.3
	Итого	4	
4 Построение защищенных распределенных систем на основе беспроводных сетей	Специфика частотного регулирования. Основные принципы проектирования защищенных беспроводных сетей. Создание аутентификационной инфраструктуры. Применение криптографических алгоритмов. Применение инфраструктуры открытых ключей (PKI);	4	ПСК-10.2, ПСК-10.4
	Итого	4	
5 Методика испытаний систем беспроводной связи	Факторы, определяющие реальную производительность системы при беспроводной передаче данныхРекомендуемый комплекс полевых испытанийОбразцовые тесты и результаты лабораторных испытанийМетодика тестирования оценки уровня защищенности.	4	ПСК-10.2, ПСК-10.3
	Итого	4	
Итого за семестр		18	

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
Предшествующие дисциплины					
1 Администрирование сетей ЭВМ	+				
2 Моделирование систем и сетей телекоммуникаций				+	
Последующие дисциплины					
1 Измерения в телекоммуникационных системах		+			
2 Информационная безопасность телекоммуникационных систем			+		
3 Проектирование защищенных телекоммуникационных систем					+

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	
ПСК-10.4	+	+	+	Домашнее задание, Конспект самоподготовки, Проверка контрольных работ, Отчет по лабораторной работе, Выступление (доклад) на занятии
ПСК-10.3	+		+	Контрольная работа, Домашнее задание, Экзамен, Конспект самоподготовки, Выступление (доклад) на занятии
ПСК-10.2	+	+	+	Контрольная работа, Домашнее задание, Экзамен, Конспект самоподготовки, Проверка контрольных работ, Отчет по лабораторной работе, Опрос на занятиях, Выступление (доклад) на занятии, Реферат

6. Интерактивные методы и формы организации обучения

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

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

Методы	Интерактивные лекции	Интерактивные лабораторные занятия	Всего
8 семестр			
Презентации с использованием интерактивной доски с обсуждением	2		2
Разработка проекта		4	4
Презентации с использованием слайдов с обсуждением	4		4
Работа в команде		6	6
Итого за семестр:	6	10	16
Итого	6	10	16

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			
2 Принципы передачи информации в радиоэфире	Построение распределенной системы беспроводной связи	6	ПСК-10.2
	Итого	6	
3 Виды беспроводных сетей. Основные угрозы информационной безопасности	Методы защиты от подслушивания в системах беспроводной связи.	6	ПСК-10.4, ПСК-10.2
	Угроза типа "Отказ в обслуживании". Способы защиты	6	
	Устройства глушения беспроводной связи	6	
	Итого	18	
4 Построение защищенных распределенных систем на основе беспроводных сетей	Криптозащита в системах беспроводной связи	6	ПСК-10.2, ПСК-10.4
	Итого	6	
5 Методика испытаний систем беспроводной связи	Проведение оценки защищенности системы беспроводной связи	6	ПСК-10.2
	Итого	6	
Итого за семестр		36	

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
8 семестр				
1 Основы и особенности беспроводных технологий	Написание рефератов	4	ПСК-10.2, ПСК-10.3	Выступление (доклад) на занятии, Домашнее задание, Опрос на занятиях, Реферат
	Проработка лекционного материала	2		
	Проработка лекционного материала	2		
	Итого	8		
2 Принципы передачи информации в радиоэфире	Проработка лекционного материала	1	ПСК-10.3, ПСК-10.4	Выступление (доклад) на занятии, Домашнее задание
	Проработка лекционного материала	2		
	Итого	3		
3 Виды беспроводных сетей. Основные угрозы информационной безопасности	Проработка лекционного материала	1	ПСК-10.2, ПСК-10.3, ПСК-10.4	Выступление (доклад) на занятии, Контрольная работа, Отчет по лабораторной работе
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	20		
	Итого	23		
4 Построение защищенных распределенных систем на основе беспроводных сетей	Проработка лекционного материала	2	ПСК-10.2, ПСК-10.4, ПСК-10.3	Выступление (доклад) на занятии, Конспект самоподготовки, Отчет по лабораторной работе, Проверка контрольных работ
	Проработка лекционного материала	4		
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	6		
	Итого	13		
5 Методика испытаний систем беспроводной связи	Проработка лекционного материала	1	ПСК-10.2, ПСК-10.3	Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	6		
	Итого	7		
Итого за семестр		54		

	Подготовка и сдача экзамена	36		Экзамен
Итого		90		

9.1. Темы рефератов

1. Протоколы безопасности беспроводных сетей
2. Аутентификация в беспроводных сетях
3. Механизмы шифрования в системах беспроводной связи

10. Курсовая работа (проект)

Не предусмотрено РУП

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				
Выступление (доклад) на занятии		5		5
Домашнее задание		5		5
Контрольная работа		5	10	15
Опрос на занятиях	5	5		10
Отчет по лабораторной работе	10	10	10	30
Реферат		5		5
Итого максимум за период	15	35	20	70
Экзамен				30
Нарастающим итогом	15	50	70	100

11.2. Пересчет баллов в оценки за контрольные точки

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

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

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

11.3. Пересчет суммы баллов в традиционную и международную оценку

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

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

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)

5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	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. Максим, М. Безопасность беспроводных сетей : Пер. с англ. / М. Максим, Д. Поллино. - М. : АйТи, 2004 ; М. : ДМК Пресс, 2004. - 281[7] с.: Библиотека ТУСУР, (наличие в библиотеке ТУСУР - 10 экз.)

12.2. Дополнительная литература

1. Барнс, К. Защита от хакеров беспроводных сетей. [Электронный ресурс] / К. Барнс, Т. Боутс, Д. Лойд, Э. Уле. — - М. : Академия АйТи, 2005 ; М. : ДМК-Пресс, 2005. - 476[4] с. (наличие в библиотеке ТУСУР - 1 экз.)
2. Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5262, дата обращения: 16.06.2017.

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Исхаков А.Ю. Защита информации в системах беспроводной связи: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_prot_wireless.zip [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_prot_wireless.zip
2. Исхаков А.Ю. Защита информации в системах беспроводной связи: методические указания для выполнения лабораторных работ для студентов специальности 10.05.02 "Информационная безопасность телекоммуникационных систем" [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_networks_lab.zip [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_networks_lab.zip

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. 1. http://www.iqlib.ru - электронная интернет библиотека;

2. 2. http://www.biblioclub.ru – полнотекстовая электронная библиотека;
3. 3. http://www.elibrary.ru - научная электронная библиотека;
4. 4. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
5. 5. http://www.sec.ru – каталог организаций в сфере информационной безопасности

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 лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 808. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Аудиосистема – 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор Optoma – 1 шт.; Компьютер лекционный ASUS ASRock AMD E2-1800/4 ГБ – 1 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 7 SP1; Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.2. Материально-техническое обеспечение для лабораторных работ

Для проведения практических (семинарских) занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 407. Состав оборудования: Учебная мебель; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже плата Gigabyte GA-H55M-S2mATX/ Intel Original Soc-1156 Core i3 3.06 GHz/ DDR III Kingston CL9 - 2 штуки по 2048 Mb/ SATA-II 250Gb Hitachi / 1024 Mb GeForse GT240 PCI-E. с широкополосным доступом в Internet, – 6 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP3; Visual Studio 2010; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. 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 сфор-

мированности 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 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.

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

Защита информации в системах беспроводной связи

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль): **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **4**
Семестр: **8**

Учебный план набора 2016 года

Разработчики:
- инженер каф. БИС А. Ю. Исхаков
- доцент каф. БИС О. О. Евсютин

Экзамен: 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
ПСК-10.4	способностью применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации	Должен знать технологии беспроводной передачи данных; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений. ; Должен уметь применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в беспроводных сетях передачи данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов.; Должен владеть навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений.;
ПСК-10.3	способностью оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации	
ПСК-10.2	способностью формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем	

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

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

Показатели и критерии	Знать	Уметь	Владеть

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

2 Реализация компетенций

2.1 Компетенция ПСК-10.4

ПСК-10.4: способностью применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой 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	защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений, перехвата информации	применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации и закрытия возможных каналов ее перехвата в беспроводных сетях передачи данных	навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
Виды занятий	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Интерактивные лекции; • Интерактивные лабораторные занятия;	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Интерактивные лекции; • Интерактивные лабораторные занятия;	• Самостоятельная работа; • Лабораторные работы; • Интерактивные лабораторные занятия;
Используемые средства оценивания	• Домашнее задание; • Конспект самоподготовки; • Отчет по лабораторной работе; • Выступление (доклад) на занятии; • Экзамен;	• Домашнее задание; • Конспект самоподготовки; • Отчет по лабораторной работе; • Выступление (доклад) на занятии; • Экзамен;	• Домашнее задание; • Отчет по лабораторной работе; • Выступление (доклад) на занятии; • Экзамен;

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

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает особенности применения защитных механизмов и средств обеспечения сетевой безопасности, свободно ориентируется в применении средств и методов предотвращения и обнаружения вторжений, перехвата информации.;	• Умеет применять защищенные протоколы, конфигурировать межсетевые экраны и средства обнаружения вторжений для защиты информации и закрытия возможных каналов ее перехвата в беспроводных сетях передачи данных;	• Владеет навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;;
Хорошо (базовый уровень)	• Знает основные средства и методы предотвращения и обнаружения вторжений, перехвата информации.;	• Умеет применять на практике основные средства защиты информации и закрытия возможных каналов перехвата акустической речевой информации в беспроводных сетях передачи данных;	• Владеет навыками управления локальной сетью, реализации сетевых протоколов с помощью программных средств;
Удовлетворительно (пороговый уровень)	• Имеет представление об основных средствах и методах предотвращения и обнаружения вторжений, перехвата информации.;	• Имеет представление о применении на практике основных средства защиты информации и закрытия возможных каналов ее перехвата акустической речевой информации в беспроводных сетях передачи данных;	• В общих понятиях владеет навыками конфигурирования локальных сетей, настройки межсетевых экранов;

2.2 Компетенция ПСК-10.3

ПСК-10.3: способностью оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации.

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	основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; принципы построения защищенных телекоммуникационных систем; механизмы реали-	оценивать возможности средств технических разведок в отношении к информации в системах беспроводной связи; противодействовать угрозам безопасности систем беспроводной связи;	методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений, разведок в отношении к системам связи, управления и объектам информатизации;

	зации атак в компьютерных сетях;		
Виды занятий	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Интерактивные лекции; • Интерактивные лабораторные занятия;	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Интерактивные лекции; • Интерактивные лабораторные занятия;	• Самостоятельная работа; • Лабораторные работы; • Интерактивные лабораторные занятия;
Используемые средства оценивания	• Контрольная работа; • Домашнее задание; • Конспект самоподготовки; • Выступление (доклад) на занятии; • Экзамен;	• Контрольная работа; • Домашнее задание; • Конспект самоподготовки; • Выступление (доклад) на занятии; • Экзамен;	• Домашнее задание; • Выступление (доклад) на занятии; • Экзамен;

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

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знать основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем, ориентироваться в принципах построения защищенных телекоммуникационных систем, механизмах реализации атак в компьютерных сетях;	• Уметь применять результаты оценки применения технических разведок в отношении к информации в системах беспроводной связи для построения систем противодействия угрозам безопасности систем беспроводной связи.;	• Владеет методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений, разведок в отношении к системам связи, управления и объектам информатизации.;
Хорошо (базовый уровень)	• Знать основные основные нормативно правовые акты и принципы построения защищенных телекоммуникационных систем ;	• Уметь распознавать средства технических разведок в отношении к информационных систем и противодействовать угрозам безопасности систем беспроводной связи.;	• Владеет навыками анализа результатов работы средств обнаружения вторжений, разведок в отношении к системам связи, управления и объектам информатизации.;
Удовлетворительно (пороговый уровень)	• Иметь представление об основных принципах построения защищенных телекоммуникационных систем и механизмах реализации атак в компьютерных сетях;	• Уметь противодействовать угрозам безопасности систем беспроводной связи на практике.;	• Имеет представление о применении на практике средств обнаружения вторжения и анализе их результатов работы;

2.3 Компетенция ПСК-10.2

ПСК-10.2: способностью формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 7.

Таблица 7 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	технологии беспроводной передачи данных; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий;	применять механизмы противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов.	навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем
Виды занятий	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Интерактивные лекции; • Интерактивные лабораторные занятия;	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Интерактивные лекции; • Интерактивные лабораторные занятия;	• Самостоятельная работа; • Лабораторные работы; • Интерактивные лабораторные занятия;
Используемые средства оценивания	• Контрольная работа; • Домашнее задание; • Конспект самоподготовки; • Отчет по лабораторной работе; • Опрос на занятиях; • Выступление (доклад) на занятии; • Реферат; • Экзамен;	• Контрольная работа; • Домашнее задание; • Конспект самоподготовки; • Отчет по лабораторной работе; • Опрос на занятиях; • Выступление (доклад) на занятии; • Реферат; • Экзамен;	• Отчет по лабораторной работе; • Домашнее задание; • Выступление (доклад) на занятии; • Реферат; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 8.

Таблица 8 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает и ориентируется в технологиях беспроводной передачи данных, а также в основных стандартах в области инфокоммуникационных систем и технологий;	• Владеть навыками применения механизмов противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	• Владеть навыками разработки технического задания для разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем;

		в соответствии с требованиями нормативно правовых актов и нормативных методических документов;	
Хорошо (базовый уровень)	• Знает основные технологии беспроводной передачи данных и стандарты в области инфокоммуникационных систем и технологий;	• Уметь применять основные механизмы противодействия нарушениям сетевой безопасности, программные и аппаратные средства защиты;	• Владеть навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем;
Удовлетворительно (пороговый уровень)	• Имеет представление о наиболее значимых технологиях и стандартах в области инфокоммуникационных систем и технологий;	• Уметь использовать программные и аппаратные средств защиты в соответствии с особенностями защищаемого объекта;	• Владеть основами нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем;

3 Типовые контрольные задания

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

3.1 Вопросы на самоподготовку

- Классификация угроз безопасности в системах беспроводной связи.
- Протоколы безопасности беспроводных сетей.
- Механизмы аутентификации в беспроводных сетях.

3.2 Темы рефератов

- Протоколы безопасности беспроводных сетей
- Аутентификация в беспроводных сетях
- Механизмы шифрования в системах беспроводной связи

3.3 Темы домашних заданий

- Особенности применения беспроводных технологий для выделенного объекта защиты.
- Выявление угроз при передаче информации в радиоэфире в системах беспроводной связи.

3.4 Темы контрольных работ

- Виды беспроводных сетей;
- Угрозы информационной безопасности в системах беспроводной связи;
- Построение защищенных распределенных систем на основе беспроводных сетей

3.5 Темы опросов на занятиях

- Протоколы безопасности беспроводных сетей
- Аутентификация в беспроводных сетях
- Механизмы шифрования в системах беспроводной связи

3.6 Темы докладов

- Протоколы безопасности беспроводных сетей
- Аутентификация в беспроводных сетях
- Механизмы шифрования в системах беспроводной связи

3.7 Темы контрольных работ

- Виды беспроводных сетей;
- Угрозы информационной безопасности в системах беспроводной связи;
- Построение защищенных распределенных систем на основе беспроводных сетей

3.8 Экзаменационные вопросы

- 1. Что стандартизирует модель OSI?
- 2. Можно ли представить еще один вариант модели взаимодействия открытых систем с другим количеством уровней, например 8 или 5?
- 3. Ниже перечислены оригинальные (англоязычные) названия семи уровней модели OSI. Отметьте, какие из названий уровней не соответствуют стандарту?
- physical layer, data-link layer, network layer, transport layer, seances layer, presentation layer, application layer
- 4. Какие из приведенных утверждений вы считаете ошибочными:
- — протокол — это программный модуль, решающий задачу взаимодействия систем;
- — протокол — это формализованное описание правил взаимодействия, включающих последовательность обмена сообщениями и их форматы;
- — термины «интерфейс» и «протокол», в сущности, являются синонимами.
- 5. На каком уровне модели OSI работает прикладная программа?
- 6. Как вы считаете, протоколы транспортного уровня устанавливаются только на конечных узлах, только на промежуточном коммуникационном оборудовании (маршрутизаторах) или и там, и там?
- 7. На каком уровне модели OSI работают сетевые службы?
- 8. Ниже перечислены некоторые сетевые устройства:
- — маршрутизатор;
- — коммутатор;
- — мост;
- — повторитель;
- — сетевой адаптер;
- — концентратор.
- В каком из этих устройств реализуются функции физического уровня модели OSI? Канального уровня? Сетевого уровня?
- 9. Какое название традиционно используется для единицы передаваемых данных на каждом из уровней OSI?
- 10. Дайте определение открытой системы.
- 11. Пусть малоизвестная небольшая компания предлагает нужный вам продукт с характеристиками, превосходящими характеристики аналогичных продуктов известных фирм. В каком из перечисленных вариантов ваши действия можно считать согласующимися с принципом открытых систем:
- — приму предложение, проверив прилагаемую документацию и убедившись, что в ней указаны характеристики, превосходящие известные аналоги;
- — приму предложение только после того, как проведу тестирование и удостоверюсь, что характеристики действительно лучше;
- — в любом случае откажусь в пользу продукта известной фирмы, так как последняя наверняка следует стандартам, а значит, будет меньше проблем с совместимостью;
- — откажусь от продукта неизвестной компании, так как есть риск ее исчезновения, а значит, могут быть проблемы с поддержкой.
- 12. Какая организация разработала стандарты сетей Ethernet?
- 13. Какое из административных подразделений Интернета непосредственно занимается стандартизацией?
- 14. Какие из перечисленных терминов являются синонимами:
- — стандарт;

– — спецификация;
– — RFC;
– — Никакие.
– 15. К какому типу стандартов могут относиться современные документы RFC:
– — к стандартам отдельных фирм;
– — к государственным стандартам;
– — к национальным стандартам;
– — к международным стандартам.
– 16. Какая организация стояла у истоков создания и стандартизации стека TCP/IP?
– 17. Определите основные особенности стека TCP/IP.
– 18. Сравните функции самых нижних уровней моделей TCP/IP и OSI.
– 19. Дайте определение транспортных и информационных услуг.
– 20. Какие протоколы относятся к слою управления (control plane)? А к слою менеджмента (management plane)?
– 21. Должны ли маршрутизаторами поддерживаться протоколы
– транспортного уровня?
– 22. Пусть на двух компьютерах установлено идентичное программное и аппаратное обеспечение за исключением того, что драйверы сетевых адаптеров Ethernet поддерживают отличающиеся интерфейсы с протоколом сетевого уровня IP. Будут ли эти компьютеры нормально взаимодействовать, если их соединить в сеть?
– 23. Как организовать взаимодействие двух компьютеров, если у них отличаются протоколы:
– — физического и канального уровней;
– — сетевого уровня;
– — прикладного уровня.
– 24. Опишите ваши действия в случае, если вам необходимо проверить, на каком этапе находится процесс стандартизации технологии MPLS?

3.9 Темы лабораторных работ

– Методы защиты от подслушивания в системах беспроводной связи.
– Угроза типа "Отказ в обслуживании". Способы защиты
– Устройства глушения беспроводной связи
– Криптозащита в системах беспроводной связи
– Построение распределенной системы беспроводной связи
– Проведение оценки защищенности системы беспроводной связи

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. Максим, М. Безопасность беспроводных сетей : Пер. с англ. / М. Максим, Д. Поллино. - М. : АйТи, 2004 ; М. : ДМК Пресс, 2004. - 281[7] с.: Библиотека ТУСУР, (наличие в библиотеке ТУСУР - 10 экз.)

4.2. Дополнительная литература

1. Барнс, К. Защита от хакеров беспроводных сетей. [Электронный ресурс] / К. Барнс, Т. Боутс, Д. Лойд, Э. Уле. — - М. : Академия АйТи, 2005 ; М. : ДМК-Пресс, 2005. - 476[4] с. (наличие в библиотеке ТУСУР - 1 экз.)

2. Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа:

https://edu.tusur.ru/publications/5262, свободный.

4.3. Обязательные учебно-методические пособия

1. Исхаков А.Ю. Защита информации в системах беспроводной связи: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_prot_wireless.zip [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_prot_wireless.zip
2. Исхаков А.Ю. Защита информации в системах беспроводной связи: методические указания для выполнения лабораторных работ для студентов специальности 10.05.02 "Информационная безопасность телекоммуникационных систем" [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_networks_lab.zip [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_networks_lab.zip

4.4. Базы данных, информационно справочные и поисковые системы

1. 1. http://www.iqlib.ru - электронная интернет библиотека;
2. 2. http://www.biblioclub.ru – полнотекстовая электронная библиотека;
3. 3. http://www.elibrary.ru - научная электронная библиотека;
4. 4. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
5. 5. http://www.sec.ru – каталог организаций в сфере информационной безопасности