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

Информационная безопасность телекоммуникационных систем

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: **5**
Семестр: **10**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Практические занятия	36	36	часов
3	Лабораторные работы	16	16	часов
4	Всего аудиторных занятий	88	88	часов
5	Из них в интерактивной форме	24	24	часов
6	Самостоятельная работа	56	56	часов
7	Всего (без экзамена)	144	144	часов
8	Подготовка и сдача экзамена	36	36	часов
9	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е

Экзамен: 10 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «25» 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:

м.н.с. каф. КИБЭВС _____ С. 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:

ст. преподаватель кафедра
КИБЭВС _____ Г. А. Праскурин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

заложить терминологический фундамент;

рассмотреть особенности построения телекоммуникационных систем;

приобрести навыки аудита телекоммуникационных систем;

научить правильно проводить оценку рисков информационной безопасности для телекоммуникационных систем;

изучить методы и средства обеспечения информационной безопасности телекоммуникационных систем;

рассмотреть основные общеметодологические принципы построения системы защиты информации для телекоммуникационных систем.

1.2. Задачи дисциплины

- ознакомление студентов с основными особенностями телекоммуникационных систем;
- развитие мышления студентов;
- обучение выявлению причин, видов, каналов утечки и искажения информации в телекоммуникационных системах;
- изучение методов и средств обеспечения информационной безопасности телекоммуникационных систем;
- исследование систем защиты информации для телекоммуникационных систем.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность телекоммуникационных систем» (Б1.Б.37) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Защита информации в системах беспроводной связи, Измерения в телекоммуникационных системах, Криптографические методы защиты информации, Основы информационной безопасности, Программно-аппаратные средства обеспечения информационной безопасности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-1 способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем;
- ПК-6 способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду;
- ПК-10 способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений;
- ПК-15 способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания;

В результате изучения дисциплины студент должен:

- **знать** принципы построения и функционирования, реализации современных телекоммуникационных систем, основных протоколов телекоммуникационных систем; последовательность и содержание этапов построения телекоммуникационных систем; эталонную модель взаимодействия открытых систем; основные криптографические методы, алгоритмов, протоколов, используемых для обеспечения безопасности в телекоммуникационных системах; модели угроз и модели нарушителя информационной безопасности телекоммуникационных систем; сущность и значение информации в развитии современного общества, применение достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в телекоммуникационных системах.
- **уметь** проводить синтез и анализ проектных решений по обеспечению безопасности

телекоммуникационных систем; моделировать информационные процессы и реорганизовывать информационные процессы; проектировать и администрировать телекоммуникационные системы; реализовывать политику безопасности телекоммуникационных систем; эффективно использовать различные методы и средства защиты информации для телекоммуникационных систем; проводить мониторинг угроз безопасности телекоммуникационных систем.

– **владеть** навыками написания аналитических справок, обзоров и прогнозов, методами и программными средствами обработки информации, способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы, способностью разрабатывать планы, программы и методики, входящие в состав технической и эксплуатационной документации; навыками составления и оформления материалов для экспертных заключений и отчетов, способностью выполнять работы по стандартизации и сертификации сетевых процессов, средств технологического оснащения, автоматизации и управления сетевым оборудованием; навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, телекоммуникационных систем, программных систем с учетом требований по обеспечению информационной безопасности; навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности, навыками использования программно-аппаратных средств обеспечения безопасности телекоммуникационных систем; способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения телекоммуникационных систем; способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 5.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		10 семестр
Аудиторные занятия (всего)	88	88
Лекции	36	36
Практические занятия	36	36
Лабораторные работы	16	16
Из них в интерактивной форме	24	24
Самостоятельная работа (всего)	56	56
Оформление отчетов по лабораторным работам	10	10
Подготовка к лабораторным работам	12	12
Проработка лекционного материала	10	10
Самостоятельное изучение тем (вопросов) теоретической части курса	12	12
Подготовка к практическим занятиям, семинарам	12	12
Всего (без экзамена)	144	144
Подготовка и сдача экзамена	36	36
Общая трудоемкость ч	180	180
Зачетные Единицы	5.0	5.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
10 семестр						
1 Введение	4	0	0	2	6	ПК-1
2 Основы построения и функционирования современных телекоммуникационных систем	4	4	0	3	11	ПК-1, ПК-15
3 Основные понятия и цели обеспечения безопасности телекоммуникационных систем	4	4	0	3	11	ПК-1, ПК-10, ПК-6
4 Угрозы информационной безопасности телекоммуникационных систем	6	6	4	16	32	ПК-1, ПК-10, ПК-6
5 Методы анализа уязвимостей телекоммуникационных систем	6	8	12	24	50	ПК-1, ПК-10, ПК-15, ПК-6
6 Методы, способы и средства защиты информации в телекоммуникационных системах	12	14	0	8	34	ПК-1, ПК-10, ПК-15, ПК-6
Итого за семестр	36	36	16	56	144	
Итого	36	36	16	56	144	

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
10 семестр			
1 Введение	Обзор содержания курса, правовые аспекты защиты информации, краткий обзор по развитию систем защиты информации, методические указания по изучению курса.	4	ПК-1
	Итого	4	
2 Основы построения и функционирования современных телекоммуникационных систем	Этапы построения телекоммуникационных систем. Эталонная модель взаимодействия открытых систем. Основные протоколы телекоммуникационных систем.	4	ПК-1, ПК-15

	Итого	4	
3 Основные понятия и цели обеспечения безопасности телекоммуникационных систем	Понятие безопасности телекоммуникационных систем. Основные цели защиты информации. Основные направления защиты телекоммуникационных систем.	4	ПК-1
	Итого	4	
4 Угрозы информационной безопасности телекоммуникационных систем	Понятие угрозы. Виды угроз и характер их происхождения. Источники и предпосылки появления угроз. Классы каналов несанкционированного получения информации. Потенциально возможные действия нарушителя. Построение модели угроз.	6	ПК-1
	Итого	6	
5 Методы анализа уязвимостей телекоммуникационных систем	Понятие риска в информационной безопасности. Выбор параметров для количественного анализа рисков в телекоммуникационных системах. Определение видов ущерба. Технологии обнаружения вторжений. Технические и программные средства анализа защищенности телекоммуникационных систем. Сертификационные и аттестационные испытания.	6	ПК-10, ПК-15
	Итого	6	
6 Методы, способы и средства защиты информации в телекоммуникационных системах	Виды побочных каналов, оценка возможности утечки информации, основные методы защиты информации от утечки по побочным каналам.	4	ПК-1, ПК-6, ПК-15
	Понятия субъекта и объекта доступа, их взаимодействие в информационном обмене. Идентификация, аутентификация, авторизация в телекоммуникационных системах.	2	
	Математическая модель систем шифрования. Основные категории стойкости. Совершенная криптосистема. Понятие о расстоянии единственности. Классификация шифров. Блоковые шифры, потоковые шифры, шифрование речевых сигналов. Криптосистемы с открытым ключом. Гибридные шифры.	4	
	Технические и программные средства сбора информации о состоянии объектов телекоммуникационных систем. Работа с данными: агрегация, поиск общих атрибутов (корреляция). Средства оповещения и отображения. Сред-	2	

	ства экспертного анализа.		
	Итого	12	
Итого за семестр		36	

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

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

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин					
	1	2	3	4	5	6
Предшествующие дисциплины						
1 Защита информации в системах беспроводной связи		+				
2 Измерения в телекоммуникационных системах		+				
3 Криптографические методы защиты информации						+
4 Основы информационной безопасности				+		
5 Программно-аппаратные средства обеспечения 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	Практические занятия	Лабораторные работы	Самостоятельная работа	
ПК-1	+	+	+	+	Контрольная работа, Экзамен, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях
ПК-6	+	+	+	+	Контрольная работа, Экзамен, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях

ПК-10	+	+	+	+	Контрольная работа, Экзамен, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях
ПК-15	+	+	+	+	Контрольная работа, Экзамен, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях

6. Интерактивные методы и формы организации обучения

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

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

Методы	Интерактивные практические занятия	Интерактивные лабораторные занятия	Интерактивные лекции	Всего
10 семестр				
Презентации с использованием слайдов с обсуждением			6	6
Разработка проекта	4	4		8
Презентации с использованием раздаточных материалов с обсуждением			4	4
Решение ситуационных задач	4			4
Работа в команде	2			2
Итого за семестр:	10	4	10	24
Итого	10	4	10	24

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
10 семестр			
4 Угрозы информационной безопасности телекоммуникационных систем	Исследование телекоммуникационной системы как объекта защиты	4	ПК-1, ПК-10
	Итого	4	
5 Методы анализа уязвимостей телекоммуникационных систем	Выявление уязвимостей телекоммуникационной системы	12	ПК-15, ПК-6
	Итого	12	
Итого за семестр		16	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
10 семестр			
2 Основы построения и функционирования современных телекоммуникационных систем	Примеры построения телекоммуникационных систем. Рассмотрение модели взаимодействия открытых систем на практике. Изучение основных протоколов, используемых в телекоммуникационных системах.	4	ПК-1
	Итого	4	
3 Основные понятия и цели обеспечения безопасности телекоммуникационных систем	Систематизация знаний об основных направлениях защиты телекоммуникационных систем: формирование целей и составления технических заданий на разработку систем защиты.	4	ПК-1, ПК-10, ПК-6
	Итого	4	
4 Угрозы информационной безопасности телекоммуникационных систем	Исследование объекта: определение потенциальных угроз, характера их происхождения, источников и предпосылок.	2	ПК-10, ПК-6
	Анализ потенциально возможных действий нарушителя. Построение модели угроз.	4	
	Итого	6	
5 Методы анализа уязвимостей телекоммуникационных систем	Анализ рисков в телекоммуникационных системах.	2	ПК-1, ПК-10, ПК-15
	Изучение современных аппаратных и программных средствами анализа уязвимостей.	6	
	Итого	8	
6 Методы, способы и средства защиты информации в телекоммуникационных системах	Защита информации от утечки по побочным каналам.	4	ПК-6, ПК-1, ПК-10, ПК-15
	Взаимодействие субъекта и объекта доступа в информационном обмене.	2	
	Применение современных методов криптозащиты в телекоммукационных системах.	4	
	Современные средства сбора и анализа информации о состоянии телекоммуникационных систем.	4	
	Итого	14	

Итого за семестр		36	

9. Самостоятельная работа

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

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
10 семестр				
1 Введение	Проработка лекционного материала	2	ПК-1	Опрос на занятиях, Экзамен
	Итого	2		
2 Основы построения и функционирования современных телекоммуникационных систем	Самостоятельное изучение тем (вопросов) теоретической части курса	2	ПК-1, ПК-15	Контрольная работа, Опрос на занятиях, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
3 Основные понятия и цели обеспечения безопасности телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	2	ПК-1, ПК-10, ПК-6	Контрольная работа, Опрос на занятиях, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
4 Угрозы информационной безопасности телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	2	ПК-10, ПК-1	Защита отчета, Контрольная работа, Опрос на занятиях, Отчет по лабораторной работе, Экзамен
	Самостоятельное изучение тем (вопросов) теоретической части курса	4		
	Проработка лекционного материала	2		
	Подготовка к лабораторным работам	4		
	Оформление отчетов по лабораторным работам	4		
	Итого	16		
5 Методы анализа уязвимостей телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-15, ПК-1, ПК-10, ПК-6	Защита отчета, Контрольная работа, Опрос на занятиях, Отчет по лабораторной работе, Экзамен
	Самостоятельное изучение тем (вопросов) теоретической части курса	4		

	Проработка лекционного материала	2		
	Подготовка к лабораторным работам	8		
	Оформление отчетов по лабораторным работам	6		
	Итого	24		
6 Методы, способы и средства защиты информации в телекоммуникационных системах	Подготовка к практическим занятиям, семинарам	4	ПК-6, ПК-1, ПК-15	Контрольная работа, Опрос на занятиях, Экзамен
	Самостоятельное изучение тем (вопросов) теоретической части курса	2		
	Проработка лекционного материала	2		
	Итого	8		
Итого за семестр		56		
	Подготовка и сдача экзамена	36		Экзамен
Итого		92		

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
10 семестр				
Контрольная работа		15	15	30
Опрос на занятиях	5	5	5	15
Отчет по лабораторной работе		10	15	25
Итого максимум за период	5	30	35	70
Экзамен				30
Нарастающим итогом	5	35	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. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. — 4-е изд. — СПб.: ПИТЕР, 2013. — 944 с. (наличие в библиотеке ТУСУР - 20 экз.)

12.2. Дополнительная литература

1. Титов А.А. Инженерно-техническая защита информации: учебное пособие. — Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010. – 197 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/654, дата обращения: 25.06.2017.

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Исхаков С.Ю. Информационная безопасность телекоммуникационных систем: методические указания для выполнения практических, самостоятельных и лабораторных работ для студентов специальности 10.05.02 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_sy_ibtks.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, 4 этаж, ауд. 401. Состав оборудования: Учебная мебель; Экран - 1 шт.; Аудиосистема – 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор – 1 шт.; Компьютер лекционный – 1 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 7 SP1; Microsoft Powerpoint Viewer.

13.1.2. Материально-техническое обеспечение для практических занятий

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 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.

13.1.4. 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 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

Информационная безопасность телекоммуникационных систем

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: **5**
Семестр: **10**

Учебный план набора 2016 года

Разработчики:
- м.н.с. каф. КИБЭВС С. Ю. Исхаков
- доцент каф. БИС О. О. Евсютин

Экзамен: 10 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
ПК-1	способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем	Должен знать принципы построения и функционирования, реализации современных телекоммуникационных систем, основных протоколов телекоммуникационных систем; последовательность и содержание этапов построения телекоммуникационных систем; эталонную модель взаимодействия открытых систем; основные криптографические методы, алгоритмов, протоколов, используемых для обеспечения безопасности в телекоммуникационных системах; модели угроз и модели нарушителя информационной безопасности телекоммуникационных систем; сущность и значение информации в развитии современного общества, применение достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в телекоммуникационных системах.; Должен уметь проводить синтез и анализ проектных решений по обеспечению безопасности телекоммуникационных систем; моделировать информационные процессы и реорганизовывать информационные процессы; проектировать и администрировать телекоммуникационные системы; реализовывать политику безопасности телекоммуникационных систем; эффективно использовать различные методы и средства защиты информации для телекоммуникационных систем; проводить мониторинг угроз безопасности телекоммуникационных систем.; Должен владеть навыками написания аналитических справок, обзоров и прогнозов, методами и программными средствами обработки информации, способностью взаимодействовать со службами информационных технологий
ПК-6	способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду	
ПК-10	способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений	
ПК-15	способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания	

		и эффективно использовать корпоративные информационные системы, способностью разрабатывать планы, программы и методики, входящие в состав технической и эксплуатационной документации; навыками составления и оформления материалов для экспертных заключений и отчетов, способностью выполнять работы по стандартизации и сертификации сетевых процессов, средств технологического оснащения, автоматизации и управления сетевым оборудованием; навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, телекоммуникационных систем, программных систем с учетом требований по обеспечению информационной безопасности; навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности, навыками использования программно-аппаратных средств обеспечения безопасности телекоммуникационных систем; способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения телекоммуникационных систем; способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности.;

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	Работает при прямом наблюдении

		задач	

2 Реализация компетенций

2.1 Компетенция ПК-1

ПК-1: способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем.

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

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	принцип построения и функционирования, реализации современных телекоммуникационных систем, основных протоколов телекоммуникационных систем; последовательность и содержание этапов построения телекоммуникационных систем.	проводить синтез и анализ проектных решений по обеспечению безопасности телекоммуникационных систем.	навыками написания аналитических справок, обзоров и прогнозов, методами и программными средствами обработки информации; способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы; способностью разрабатывать планы, программы и методики, входящие в состав технической и эксплуатационной документации.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Отчет по лабораторной работе; • Опрос на занятиях; • Экзамен;	• Контрольная работа; • Отчет по лабораторной работе; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • 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 принципы построения и функционирования, реализации современных телекоммуникационных систем, основные протоколы телекоммуникационных систем, последовательность и содержание этапов построения телекоммуникационных систем.;	• Умеет проводить синтез и анализ проектных решений по обеспечению безопасности телекоммуникационных систем.;	• Владеет навыками написания аналитических справок, обзоров и прогнозов, методами и программными средствами обработки информации, способностью разрабатывать планы, программы и методики, входящие в состав технической и эксплуатационной документации.;
Хорошо (базовый уровень)	• Знает основные принципы построения и функционирования, реализации современных телекоммуникационных систем, основные протоколы телекоммуникационных систем.;	• Умеет выделить основные этапы проведения анализа проектных решений по обеспечению безопасности телекоммуникационных систем.;	• Владеет основными навыками написания аналитических справок, обзоров и прогнозов, методами и программными средствами обработки информации.;
Удовлетворительно (пороговый уровень)	• Имеет общее представление об основных принципах построения и функционирования, реализации современных телекоммуникационных систем.;	• Способен в общих понятиях описать анализ проектных решений по обеспечению безопасности телекоммуникационных систем.;	• Владеет общим представлением о процессах создания аналитических справок, обзоров и прогнозов, методами и программными средствами обработки информации.;

2.2 Компетенция ПК-6

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

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

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	эталонную модель взаимодействия открытых систем; сущность и значение информации в развитии современного общества, применение достижения современных информационных технологий по профилю деятельности в телекоммуникационных системах.	моделировать информационные процессы и реорганизовывать информационные процессы; проектировать и администрировать телекоммуникационные системы.	навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, телекоммуникационных систем, программных систем с учетом требований по обеспечению информационной безопасности.

Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Отчет по лабораторной работе; • Опрос на занятиях; • Экзамен;	• Контрольная работа; • Отчет по лабораторной работе; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • 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)	• Знает и ориентируется в эталонной модели взаимодействия открытых систем, знает сущность и значение информации в развитии современного общества.;	• Умеет моделировать информационные процессы, организовывать информационные процессы, проектировать и администрировать телекоммуникационные системы.;	• Владеет навыками эксплуатации и администрирования телекоммуникационных систем, программных систем с учетом требований по обеспечению информационной безопасности.;
Хорошо (базовый уровень)	• Знает основными понятия в эталонной модели взаимодействия открытых систем, знает сущность и значение информации в развитии современного общества.;	• Умеет применять основные знания по моделированию информационных процессов, организации информационных процессов, умеет проектировать и администрировать телекоммуникационные системы.;	• Владеет основными навыками эксплуатации и администрирования телекоммуникационных систем, программных систем с учетом требований по обеспечению информационной безопасности.;
Удовлетворительно (пороговый уровень)	• Имеет общие представления об эталонной модели взаимодействия открытых систем, а также о сущности и значении информации в развитии современного общества.;	• Способен в общих понятиях описать процесс моделирования информационных процессов, организации информационных процессов, проектирования и администрирования телекоммуникационные системы.;	• Владеет общим представлением об эксплуатации и администрирования телекоммуникационных систем, программных систем с учетом требований по обеспечению информационной безопасности.;

2.3 Компетенция ПК-10

ПК-10: способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений.

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	сущность и значение информации в развитии современного общества, применение достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в телекоммуникационных системах.	реализовывать политику безопасности телекоммуникационных систем; эффективно использовать различные методы и средства защиты информации для телекоммуникационных систем.	навыками составления и оформления материалов для экспертных заключений и отчетов; способностью выполнять работы по стандартизации и сертификации сетевых процессов, средств технологического оснащения, автоматизации и управления сетевым оборудованием.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Отчет по лабораторной работе; • Опрос на занятиях; • Экзамен;	• Контрольная работа; • Отчет по лабораторной работе; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • 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 сущность и значение информации в развитии современного общества, применение достижений современных информационных технологий для поиска и обработки больших	• Умеет реализовывать политику безопасности телекоммуникационных систем, использовать различные методы и средства защиты информации для телекоммуникационных систем,	• Владеет навыками составления и оформления материалов для экспертных заключений и отчетов, способностью выполнять работы по стандартизации и сертификации сетевых

	объемов информации по профилю деятельности в телекоммуникационных системах.;	оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности.;	процессов, средств технологического оснащения, автоматизации и управления сетевым оборудованием.;
Хорошо (базовый уровень)	• Знает основные понятия в области значения информации в развитии современного общества, применения достижений современных информационных технологий по профилю деятельности в телекоммуникационных системах.;	• Умеет использовать наиболее применимые методы и средства защиты информации для телекоммуникационных систем, применять основные методы оценки выполнения требований нормативных правовых актов и нормативных методических документов в области информационной безопасности.;	• Владеет основными навыками по составлению и оформлению материалов для экспертных заключений и отчетов, способностью выполнять работы по стандартизации и сертификации средств технологического оснащения, автоматизации и управления сетевым оборудованием.;
Удовлетворительно (пороговый уровень)	• Имеет общие представления в области значения информации в развитии современного общества, применения достижений современных информационных технологий по профилю деятельности в телекоммуникационных системах.;	• Способен в общих понятиях оценить выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности.;	• Владеет общими представлениями о стандартизации и сертификации средств технологического оснащения, автоматизации и управления сетевым оборудованием.;

2.4 Компетенция ПК-15

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

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 9.

Таблица 9 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	основные криптографические методы, алгоритмов, протоколов, используемых для обеспечения безопасности в телекоммуникационных системах; модели угроз и модели нарушителя информационной безопасности телекоммуникационных систем.	проводить мониторинг угроз безопасности телекоммуникационных систем.	навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; навыками использования программно-аппаратных средств обеспечения безопасности телекоммуникационных систем; способностью проводить анализ, предла-

			гать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения телекоммуникационных систем; способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Отчет по лабораторной работе; • Опрос на занятиях; • Экзамен;	• Контрольная работа; • Отчет по лабораторной работе; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 10.

Таблица 10 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает основные криптографические методы, используемые для обеспечения безопасности в телекоммуникационных системах, а также модели угроз и модели нарушителя информационной безопасности телекоммуникационных систем.;	• Умеет проводить инструментальный мониторинг угроз безопасности телекоммуникационных систем.;	• Владеет навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности, навыками использования программно-аппаратных средств обеспечения безопасности телекоммуникационных систем, способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности при-

			менения телекоммуникационных систем.;
Хорошо (базовый уровень)	• Знает модели угроз и модели нарушителя информационной безопасности телекоммуникационных систем.;	• Умеет выделять основные этапы мониторинга угроз безопасности телекоммуникационных систем.;	• Владеет основными навыками по разработке, документированию компьютерных сетей с учетом требований по обеспечению безопасности.;
Удовлетворительно (пороговый уровень)	• Имеет общее представление о модели угроз и модели нарушителя информационной безопасности телекоммуникационных систем.;	• Способен в общих понятиях описать мониторинг угроз безопасности телекоммуникационных систем.;	• Владеет общим представление о разработке, документированию компьютерных сетей с учетом требований по обеспечению безопасности.;

3 Типовые контрольные задания

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

3.1 Темы опросов на занятиях

– Обзор содержания курса, правовые аспекты защиты информации, краткий обзор по развитию систем защиты информации, методические указания по изучению курса.

– Этапы построения телекоммуникационных систем. Эталонная модель взаимодействия открытых систем. Основные протоколы телекоммуникационных систем.

– Понятие безопасности телекоммуникационных систем. Основные цели защиты информации. Основные направления защиты телекоммуникационных систем.

– Понятие угрозы. Виды угроз и характер их происхождения. Источники и предпосылки появления угроз. Классы каналов несанкционированного получения информации. Потенциально возможные действия нарушителя. Построение модели угроз.

– Понятие риска в информационной безопасности. Выбор параметров для количественного анализа рисков в телекоммуникационных системах. Определение видов ущерба. Технологии обнаружения вторжений. Технические и программные средства анализа защищенности телекоммуникационных систем. Сертификационные и аттестационные испытания.

– Виды побочных каналов, оценка возможности утечки информации, основные методы защиты информации от утечки по побочным каналам.

– Понятия субъекта и объекта доступа, их взаимодействие в информационном обмене. Идентификация, аутентификация, авторизация в телекоммуникационных системах.

– Математическая модель систем шифрования. Основные категории стойкости. Совершенная криптосистема. Понятие о расстоянии единственности. Классификация шифров. Блоковые шифры, потоковые шифры, шифрование речевых сигналов. Криптосистемы с открытым ключом. Гибридные шифры.

– Технические и программные средства сбора информации о состоянии объектов телекоммуникационных систем. Работа с данными: агрегация, поиск общих атрибутов (корреляция). Средства оповещения и отображения. Средства экспертного анализа.

3.2 Темы контрольных работ

– Основные понятия и цели обеспечения безопасности телекоммуникационных систем.

– Исследование объекта: определение потенциальных угроз, характера их происхождения, источников и предпосылок.

3.3 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?

3.4 Темы лабораторных работ

– Исследование телекоммуникационной системы как объекта защиты
– Выявление уязвимостей телекоммуникационной системы

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. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. — 4-е изд. — СПб.: ПИТЕР, 2013. — 944 с. (наличие в библиотеке ТУСУР - 20 экз.)

4.2. Дополнительная литература

1. Титов А.А. Инженерно-техническая защита информации: учебное пособие. — Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010. – 197 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/654, свободный.

4.3. Обязательные учебно-методические пособия

1. Исхаков С.Ю. Информационная безопасность телекоммуникационных систем: методические указания для выполнения практических, самостоятельных и лабораторных работ для студентов специальности 10.05.02 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_sy_ibtks.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