МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность телекоммуникационных систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **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 2020 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	Самостоятельная работа	92	92	часов
6	Всего (без экзамена)	180	180	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	216	216	часов
		6.0	6.0	З.Е.

Экзамен: 10 семестр

Томск

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16.11.2016 года, рассмотрена и одобрена на заседании кафедры БИС «___» _____ 20__ года, протокол №_____.

Разработчик:

старший преподаватель Кафедра телекоммуникаций и основ радиотехники (ТОР) _____ Д. С. Брагин

Заведующий обеспечивающей каф. БИС _____ Е. Ю. Костюченко

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. БИС _____ Е. Ю. Костюченко

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

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.08.05) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Защита информации в системах беспроводной связи, Измерения в телекоммуникационных системах, Основы информационной безопасности, Программно-аппаратные средства обеспечения информационной безопасности, Проектирование защищенных телекоммуникационных систем, Проектная деятельность (ГПО-3).

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-5 способностью применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач;
– 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 обучающийся должен:

– **знать** - принцип построения и функционирования, реализации современных телекоммуникационных систем, основных протоколов телекоммуникационных систем; - последовательность и содержание этапов построения телекоммуникационных систем; - эталонную модель взаимодействия открытых систем; - требования нормативных правовых актов и нормативных методи-

ческих документов в области информационной безопасности при проверке защищенных телекоммуникационных систем.

– **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 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 использования программно-аппаратных средств обеспечения безопасности телекоммуникационных систем; - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения телекоммуникационных систем.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6.0 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
Самостоятельная работа (всего)	92	92
Оформление отчетов по лабораторным работам	16	16
Подготовка к лабораторным работам	8	8
Проработка лекционного материала	10	10
Самостоятельное изучение тем (вопросов) теоретической части курса	16	16
Подготовка к практическим занятиям, семинарам	42	42
Всего (без экзамена)	180	180
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	216	216
Зачетные Единицы	6.0	6.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
10 семестр						

1 Введение	4	0	0	2	6	ПК-1, ПК-10, ПК-6
2 Основы построения и функционирования современных телекоммуникационных систем	4	4	0	7	15	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6
3 Основные понятия и цели обеспечения безопасности телекоммуникационных систем	4	4	0	7	15	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6
4 Угрозы информационной безопасности телекоммуникационных систем	6	6	4	22	38	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6
5 Методы анализа уязвимостей телекоммуникационных систем	6	8	12	36	62	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6
6 Методы, способы и средства защиты информации в телекоммуникационных системах	12	14	0	18	44	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6
Итого за семестр	36	36	16	92	180	
Итого	36	36	16	92	180	

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	6	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6

	угроз.		
	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	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6
	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	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6
	Понятия субъекта и объекта доступа, их взаимодействие в информационном обмене. Идентификация, аутентификация, авторизация в телекоммуникационных системах.	2	
	Математическая модель систем шифрования-дешифрования. Основные категории стойкости. Совершенная криптосистема. Понятие о расстоянии единственности. Классификация шифров. Блоковые шифры, потоковые шифры, шифрование речевых сигналов, шифрование ГОСТ и DES.-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.Средства экспертного анализа.	2	
	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 Основы информационной безопасности	+		+	+		+
4 Программно-аппаратные средства обеспечения информационной безопасности		+	+	+	+	+
5 Проектирование защищенных телекоммуникационных систем				+	+	+
6 Проектная деятельность (ГПО-3)	+	+	+			
Последующие дисциплины						
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+	+
2 Преддипломная практика	+	+	+	+	+	+

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

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

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

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	
ОПК-5	+		+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат
ПК-1	+	+	+	+	Контрольная работа, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат
ПК-6	+	+	+	+	Контрольная работа, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат
ПК-10	+	+	+	+	Контрольная работа, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат

ПК-15	+	+	+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

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	Лабораторная работа посвящена исследованию телекоммуникационных систем как объекта защиты с целью формализованного представления модели угроз. Для выбранной телекоммуникационной системы необходимо составить ее описание как объекта защиты, провести анализ защищенности информации по следующим разделам: 1) виды угроз; 2) характер происхождения угроз; 3) источники появления угроз; 4) классы каналов несанкционированного получения информации; 5) причины нарушения целостности информации; 6) потенциально возможные злоумышленные действия. На основании полученных данных, используя эмпирический подход, необходимо построить модель угроз для выбранной телекоммуникационной системы.	4	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6
	Итого	4	
5 Методы анализа уязвимостей телекоммуникационных систем	Лабораторная работа посвящена практическому применению методов выявления уязвимостей телекоммуникационных систем. Обзор современных аппаратных и программных средств (в т.ч. дистрибутивов) для проведения разведки и сбора информации об исследуемой телекоммуникационной системе: сканирование сети, анализ защищенности сетевой инфраструктуры, анализ методов обход проактивных систем защиты. Введение в социальную инженерию.	12	ОПК-5, ПК-1, ПК-10, 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
	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
	Взаимодействие субъекта и объекта доступа в информационном обмене.	2	
	Применение современных методов криптозащиты в телекоммуникационных 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, ПК-10, ПК-6	Опрос на занятиях, Тест
	Итого	2		
2 Основы построения и функционирования современных телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-1, ОПК-5, ПК-10, ПК-15, ПК-6	Опрос на занятиях, Тест
	Самостоятельное изучение тем (вопросов) теоретической части курса	2		
	Проработка лекционного материала	1		
	Итого	7		
3 Основные понятия и цели обеспечения безопасности телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	4	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6	Опрос на занятиях, Тест
	Самостоятельное изучение тем (вопросов) теоретической части курса	2		
	Проработка лекционного материала	1		
	Итого	7		
4 Угрозы информационной безопасности телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	8	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6	Выступление (доклад) на занятии, Защита отчета, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Самостоятельное изучение тем (вопросов) теоретической части курса	6		
	Проработка лекционного материала	2		
	Подготовка к лабораторным работам	2		
	Оформление отчетов по лабораторным работам	4		
	Итого	22		
5 Методы анализа уязвимостей телекоммуникационных систем	Подготовка к практическим занятиям, семинарам	12	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6	Выступление (доклад) на занятии, Защита отчета, Опрос на занятиях, Отчет по лабораторной работе, Реферат, Тест
	Самостоятельное изучение тем (вопросов) теоретической части курса	4		
	Проработка лекционного материала	2		

	Подготовка к лабораторным работам	6		
	Оформление отчетов по лабораторным работам	12		
	Итого	36		
6 Методы, способы и средства защиты информации в телекоммуникационных системах	Подготовка к практическим занятиям, семинарам	14	ОПК-5, ПК-1, ПК-10, ПК-15, ПК-6	Выступление (доклад) на занятии, Опрос на занятиях, Тест
	Самостоятельное изучение тем (вопросов) теоретической части курса	2		
	Проработка лекционного материала	2		
	Итого	18		
Итого за семестр		92		
	Подготовка и сдача экзамена	36		Экзамен
Итого		128		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

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				
Выступление (доклад) на занятии		3	3	6
Защита отчета		7	7	14
Контрольная работа	5		5	10
Опрос на занятиях	5	5	5	15
Отчет по лабораторной работе		3	3	6
Реферат		5	5	10
Тест	3	3	3	9
Итого максимум за период	13	26	31	70
Экзамен				30
Нарастающим итогом	13	39	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. Построение защищенных корпоративных сетей [Электронный ресурс]: учебное пособие / Р.Н. Ачилов. - Электорн. дан. - Москва : ДМК Пресс, 2013. - 250 с. — Режим доступа: https://e.lanbook.com/book/66472 (дата обращения: 11.02.2021).

12.2. Дополнительная литература

1. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2015. 284 с. — Режим доступа: https://edu.tusur.ru/publications/5262 (дата обращения: 11.02.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Исхаков С.Ю. Информационная безопасность телекоммуникационных систем [Электронный ресурс]: методические указания для выполнения практических, самостоятельных и лабораторных работ для студентов специальности 10.05.02 — Режим доступа: http://kibevs.tusur.ru/default/files/upload/work_progs/iay/iskhakov_sy_ibtks.zip (дата обращения: 11.02.2021).

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

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. http://www.biblioclub.ru - полнотекстовая электронная библиотека;
2. http://www.elibrary.ru - научная электронная библиотека;
3. https://www.springer.com - издательство с доступом к реферативным и полнотекстовым материалам журналов и книг;
4. http://www.garant.ru - информационно-правовой портал;
5. https://e.lanbook.com - электронно-библиотечная система Издательства Лань.

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

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

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

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

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория Центра НТИ "Сенсорика"

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, учебная аудитория для проведения занятий семинарского типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации, помещение для самостоятельной работы

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 414 ауд.

Описание имеющегося оборудования:

Не имеется

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение не требуется.

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Аудитория Интернет-технологий и информационно-аналитической деятельности

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

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры: AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb/ мышь/ клавиатура/ монитор (15шт.);
- Компьютеры: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (6шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- GPSS Studio
- Kaspersky Endpoint Security 10 для Windows
- Microsoft SQL Server 2014
- Microsoft Windows 10
- VirtualBox
- Visio
- Visual Studio
- Специальное программное обеспечение информационных и аналитических систем ПО Spark

13.1.4. Материально-техническое и программное обеспечение для самостоятельной работы

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

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

Состав оборудования:

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

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

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

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

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

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

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

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

14.1.1. Тестовые задания

1. Что из нижеперечисленного не относится к перечню сведений конфиденциального характера, утвержденного Президентом Российской Федерации?

a) Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

b) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

c) Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

d) Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

2. Модель угроз безопасности информации не включает в себя:

a) Описание информационной системы и ее структурно-функциональных характеристик;

b) Описание угроз безопасности информации;

c) Описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы;

d) Стадии (этапы работ) создания системы защиты информационной системы.

3. При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляются:

a) Проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

b) Установка средств мониторинга сетевой инфраструктуры;

c) Разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации;

d) Внедрение документов, регламентирующих организационные меры по защите информации.

4. Анализ уязвимостей информационной системы проводится в целях:

a) Оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации;

b) Оценки эффективности использования политик разграничения доступа;

c) Оптимизации производительности программно-аппаратных средств защиты информации;

d) Сегментации информационной системы.

5. Что из нижеперечисленного не относится к международным методикам проведения тестирования на проникновение, ориентированных на моделирование атак, направленных на сетевую инфраструктуру организации:

a) Trusted Computer System Evaluation Criteria;

b) PCI DSS;

c) NIST SP800-115;

d) Open Source Security Testing Methodology Manual.

6. Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа называется:

a) Характеристика нарушителя;

b) Модель нарушителя;

c) Сценарий нарушителя;

d) Модель источников угроз.

7. Перехват данных является угрозой:

a) Доступности;

b) Конфиденциальности;

c) Целостности;

d) Достоверности.

8. Риск информационной безопасности это

a) Число уязвимостей в системе;

b) Отношение стоимости системы защиты к вероятности её «простоя»;

c) Сочетание вероятности угрозы информационной безопасности и последствий её наступления;

d) Оценка стоимости защитных средств.

9. Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации называется …

a) Угрозой безопасности;

b) Компьютерной безопасностью;

c) Анализом угроз;

d) Атакой на информационную систему.

10. Заключительным этапом построения системы защиты является …

a) Анализ уязвимых мест;

b) Планирование;

c) Обследование;

d) Сопровождение.

11. Защита информации это:

a) Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё;

b) Совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

c) Процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

d) Получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

12. Свойство доступности достигается за счет применения мер, направленных на повышение:

a) Аутентичности;

b) Непротиворечивости;

c) Отказоустойчивости;

d) Неотказуемости.

13. Получение доступа к информации субъектом в нарушение действующей политики разграничения доступа называется…

a) Несанкционированный доступ;

b) Злоумышленный доступ

c) Неразрешенный доступ;

d) Запретный доступ.

14. Набор норм, правил и практических приемов, регулирующих управление, защиту и распространение ценной информации, называется …

a) Моделью безопасности;

b) Методом шифрования;

c) Компьютерной безопасностью;

d) Политикой безопасности.

15. Выберите неверное утверждение. Сигнатурный метод выявления атак характеризуется:

a) Сравнением исследуемого объекта с ранее известными образцами-эталонами;

b) Способностью обнаруживать ранее неизвестные атаки;

c) Простотой в настройке и эксплуатации для конечного пользователя системы;

d) Популярностью использования в системах антивирусной защиты.

16. Экранирование может использоваться для:

a) Анализа рисков;

b) Предупреждения нарушений информационной безопасности;

c) Обнаружения нарушений;

d) Локализации последствий нарушений.

17. В качестве аутентификатора в сетевой среде могут использоваться:

a) Клавиатурный почерк;

b) Номер карточки пенсионного страхования;

c) Результат работы генератора одноразовых паролей;

d) PIN-код.

18. Криптография необходима для реализации следующих сервисов безопасности:

a) Идентификация;

b) Экранирование;

c) Аудит;

d) Аутентификация.

19. Сколько уровней содержит модель взаимодействия открытых систем (OSI) ?

a) 3;

b) 7;

c) 10;

d) 32.

20. Какая международная организация отвечает за выделение уникальных глобальных адресов в сети Internet?

a) IEEE;

b) ISO;

c) FDDI;

d) ICANN.

21. Что из перечисленного может быть MAC-адресом?

a) 22:16:98:15;

b) 00:1B:12:86:E4:22;

c) 00:B0:A1:8C:32:65:BB;

d) 01:23:44:55:E4:6T.

22. Token Ring – это…

a) Сетевая модель;

b) Сетевая архитектура;

c) Протокол канального уровня;

d) Протокол прикладного уровня.

23. Протоколирование и аудит могут использоваться для:

a) Обеспечения целостности информации;

b) Предупреждения нарушений информационной безопасности;

c) Реализации правил разграничения доступа;

d) Восстановления режима информационной безопасности.

24. Аутентификация на основе пароля, переданного по сети в зашифрованном виде с использованием сеансового ключа, не обеспечивает защиты от:

a) Перехвата;

b) Несанкционированного доступа;

c) Воспроизведения;

d) Атак на доступность.

25. Каковы основные функции роли "аутентификатор (Authenticator)" согласно стандарту IEEE 802.1X:

a) Управляет физическим доступом к сети, основываясь на статусе аутентификации клиента;

b) Запрашивает доступ к беспроводной локальной сети и отвечает на запросы точки доступа;

c) Выполняет фактическую аутентификацию клиента: проверяет подлинность клиента и информирует точку доступа о предоставлении или отказе клиенту в доступе к сети;

d) Инициирует процесс аутентификации.

26. Разновидность сетевой атаки типа MITM (Man in the middle), применяемая в сетях с использованием протокола ARP:

a) "ARP-spoofing";

b) "Negative ARP";

c) IPSEC;

d) VLAN-ARP.

27. Каким принципом следует руководствоваться для обеспечения информационной безопасности сетевых конфигураций?

a) Выработка и проведение в жизнь единой политики безопасности;

b) Унификация аппаратно-программных платформ;

c) Увеличение затрат на средства защиты;

d) Минимизация числа используемых приложений.

28. Выберите неверное утверждение. Сигнатурный метод выявления атак характеризуется:

a) Сравнением исследуемого объекта с ранее известными образцами-эталонами;

b) Способностью обнаруживать ранее неизвестные атаки;

c) Простотой в настройке и эксплуатации для конечного пользователя системы;

d) Популярностью использования в системах антивирусной защиты.

29. Устройство, предназначенное для защиты помещений от утечки информации по акустическим и виброканалам и специально разработанное для сеансового блокирования подслушивающих устройств, называется ?

a) Модулятор;

b) Колонка зашумления;

c) Генератор виброакустического шума;

d) Синтезатор шума.

30. Программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами, – это …

a) Межсетевой экран;

b) Коммутатор;

c) Блокирующий маршрутизатор;

d) Шлюз сеансового уровня.

14.1.2. 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?

14.1.3. Темы докладов

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-дешифрования. Основные категории стойкости. Совершенная криптосистема. Понятие о расстоянии единственности. Классификация шифров. Блоковые шифры, потоковые шифры, шифрование речевых сигналов, шифрование ГОСТ и DES. 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.

14.1.4. 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-дешифрования. Основные категории стойкости. Совершенная криптосистема. Понятие о расстоянии единственности. Классификация шифров. Блоковые шифры, потоковые шифры, шифрование речевых сигналов, шифрование ГОСТ и DES.

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.

14.1.5. Темы контрольных работ

Систематизация знаний об основных направлениях защиты телекоммуникационных систем: формирование целей и составления технических заданий на разработку систем защиты.

Изучение современных аппаратных и программных средствами анализа уязвимостей.

14.1.6. Темы рефератов

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.

14.1.7. Темы лабораторных работ

Лабораторная работа посвящена исследованию телекоммуникационных систем как объекта защиты с целью формализованного представления модели угроз. Для выбранной телекоммуникационной системы необходимо составить ее описание как объекта защиты, провести анализ защищенности информации по следующим разделам: 1) виды угроз; 2) характер происхождения угроз; 3) источники появления угроз; 4) классы каналов несанкционированного получения информации; 5) причины нарушения целостности информации; 6) потенциально возможные злоумышленные действия. На основании полученных данных, используя эмпирический подход, необходимо построить модель угроз для выбранной телекоммуникационной системы.

Лабораторная работа посвящена практическому применению методов выявления уязвимостей телекоммуникационных систем. Обзор современных аппаратных и программных средств (в т.ч. дистрибутивов) для проведения разведки и сбора информации об исследуемой телекоммуника-

ционной системе: сканирование сети, анализ защищенности сетевой инфраструктуры, анализ методов обход проактивных систем защиты. Введение в социальную инженерию.

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

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

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

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

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

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

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

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

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

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

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