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: **Управление безопасностью телекоммуникационных систем и сетей**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра безопасности информационных систем (БИС)**
Курс: **5**
Семестр: **10**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	10 семестр	Всего	Единицы
Лекционные занятия	36	36	часов
Практические занятия	36	36	часов
в т.ч. в форме практической подготовки	12	12	часов
Лабораторные занятия	20	20	часов
в т.ч. в форме практической подготовки	12	12	часов
Самостоятельная работа	88	88	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	216	216	часов
	6	6	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	10

Томск

1. Общие положения

1.1. Цели дисциплины

1. заложить терминологический фундамент.
2. рассмотреть особенности построения телекоммуникационных систем.
3. приобрести навыки аудита телекоммуникационных систем.
4. научить правильно проводить оценку рисков информационной безопасности для телекоммуникационных систем.
5. изучить методы и средства обеспечения информационной безопасности телекоммуникационных систем.
6. рассмотреть основные общеметодологические принципы построения системы защиты информации для телекоммуникационных систем.

1.2. Задачи дисциплины

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

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль специализации (major).
Индекс дисциплины: Б1.О.05.04.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

ОПК-13. Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	ОПК-13.1. Знает основные системы и сети электрической связи, включая локальные и глобальные сети, сеть «интернета вещей», принципы их построения и технические характеристики входящих в них элементов, а также основные уязвимости элементов информационно-телекоммуникационной инфраструктуры и принципы обеспечения её информационной безопасности	Перечень основных систем и сетей электрической связи, включая локальные и глобальные сети, сеть «интернета вещей», принципы их построения и технические характеристики входящих в них элементов, а также основные уязвимости элементов информационно-телекоммуникационной инфраструктуры и принципы обеспечения её информационной безопасности
	ОПК-13.2. Умеет оценивать технические возможности основных систем и сетей электрической связи и анализировать угрозы информационно-телекоммуникационной инфраструктуре и циркулирующей в ней информации, выбирать необходимые средства для обеспечения информационной безопасности	Пример оценки технических возможностей основных систем и сетей электрической связи и анализа угроз информационно-телекоммуникационной инфраструктуре и циркулирующей в ней информации, выбора необходимых средств для обеспечения информационной безопасности
	ОПК-13.3. Владеет навыком оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	Демонстрация владения навыком оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		10 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	92	92
Лекционные занятия	36	36
Практические занятия	36	36
Лабораторные занятия	20	20
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	88	88
Подготовка к тестированию	24	24
Подготовка к лабораторной работе, написание отчета	64	64
Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	216	216
Общая трудоемкость (в з.е.)	6	6

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
10 семестр						
1 Введение	4	-	-	4	8	ОПК-13
2 Основы построения и функционирования современных телекоммуникационных систем	4	4	-	4	12	ОПК-13
3 Основные понятия и цели обеспечения безопасности телекоммуникационных систем	4	4	-	4	12	ОПК-13
4 Угрозы информационной безопасности телекоммуникационных систем	6	6	6	14	32	ОПК-13
5 Методы анализа уязвимостей телекоммуникационных систем	6	8	14	58	86	ОПК-13
6 Методы, способы и средства защиты информации в телекоммуникационных системах	12	14	-	4	30	ОПК-13
Итого за семестр	36	36	20	88	180	
Итого	36	36	20	88	180	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), 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	ОПК-13
	Итого	4	
2 Основы построения и функционирования современных телекоммуникационных систем	Этапы построения телекоммуникационных систем. Эталонная модель взаимодействия открытых систем. Основные протоколы телекоммуникационных систем	4	ОПК-13
	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	ОПК-13
	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	ОПК-13
	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-13
	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-13
	Понятия субъекта и объекта доступа, их взаимодействие в информационном обмене. Идентификация, аутентификация, авторизация в телекоммуникационных системах.	2	ОПК-13
	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	ОПК-13
	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	ОПК-13
	Итого	12	
Итого за семестр		36	
Итого		36	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3 – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	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	ОПК-13
	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	ОПК-13
	Итого	4	
4 Угрозы информационной безопасности телекоммуникационных систем	Исследование объекта: определение потенциальных угроз, характера их происхождения, источников и предпосылок.	2	ОПК-13
	Анализ потенциально возможных действий нарушителя. Построение модели угроз.	4	ОПК-13
	Итого	6	
5 Методы анализа уязвимостей телекоммуникационных систем	Анализ рисков в телекоммуникационных системах.	2	ОПК-13
	Изучение современных аппаратных и программных средствами анализа уязвимостей.	6	ОПК-13
	Итого	8	
6 Методы, способы и средства защиты информации в телекоммуникационных системах	Защита информации от утечки по побочным каналам.	4	ОПК-13
	Взаимодействие субъекта и объекта доступа в информационном обмене.	2	ОПК-13
	Применение современных методов криптозащиты в телекоммуникационных системах.	4	ОПК-13
	Современные средства сбора и анализа информации о состоянии телекоммуникационных систем.	4	ОПК-13
	Итого	14	
Итого за семестр		36	
Итого		36	

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	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.	6	ОПК-13
	Итого	6	
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.	14	ОПК-13
	Итого	14	
Итого за семестр		20	
Итого		20	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
10 семестр				
1 Введение	Подготовка к тестированию	4	ОПК-13	Тестирование
	Итого	4		
2 Основы построения и функционирования современных телекоммуникационных систем	Подготовка к тестированию	4	ОПК-13	Тестирование
	Итого	4		
3 Основные понятия и цели обеспечения безопасности телекоммуникационных систем	Подготовка к тестированию	4	ОПК-13	Тестирование
	Итого	4		
4 Угрозы информационной безопасности телекоммуникационных систем	Подготовка к тестированию	4	ОПК-13	Тестирование
	Подготовка к лабораторной работе, написание отчета	10	ОПК-13	Лабораторная работа
	Итого	14		
5 Методы анализа уязвимостей телекоммуникационных систем	Подготовка к тестированию	4	ОПК-13	Тестирование
	Подготовка к лабораторной работе, написание отчета	54	ОПК-13	Лабораторная работа
	Итого	58		
6 Методы, способы и средства защиты информации в телекоммуникационных системах	Подготовка к тестированию	4	ОПК-13	Тестирование
	Итого	4		
Итого за семестр		88		
	Подготовка и сдача экзамена	36		Экзамен
Итого		124		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности				Формы контроля
	Лек. зан.	Прак. зан.	Лаб. раб.	Сам. раб.	
ОПК-13	+	+	+	+	Лабораторная работа, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	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				
Лабораторная работа	0	10	30	40
Тестирование	10	10	10	30
Экзамен				30
Итого максимум за период	10	20	40	100
Нарастающим итогом	10	30	70	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	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)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Построение защищенных корпоративных сетей [Электронный ресурс]: учебное пособие / Р.Н. Ачилов. - Электорн. дан. - Москва : ДМК Пресс, 2013. - 250 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/66472.

7.2. Дополнительная литература

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

7.3. Учебно-методические пособия

7.3.1. 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 [Электронный ресурс]: — Режим доступа: https://cloud.fb.tusur.ru/index.php/s/6nbcpnLcZSMEGn5.

7.3.2. 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.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. 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 достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для практических занятий

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:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Microsoft Windows 10;
- VirtualBox;
- Visual Studio;

8.3. 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:
- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- Microsoft Windows 10;
- VirtualBox;
- Visual Studio;

8.4. 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.

Описание имеющегося оборудования:
- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

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

8.5. 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 зрения** 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.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Введение	ОПК-13	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
2 Основы построения и функционирования современных телекоммуникационных систем	ОПК-13	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
3 Основные понятия и цели обеспечения безопасности телекоммуникационных систем	ОПК-13	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
4 Угрозы информационной безопасности телекоммуникационных систем	ОПК-13	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
5 Методы анализа уязвимостей телекоммуникационных систем	ОПК-13	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
6 Методы, способы и средства защиты информации в телекоммуникационных системах	ОПК-13	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

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;
    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.

9.1.2. Перечень экзаменационных вопросов

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 18 50017 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?

9.1.3. Темы лабораторных работ

1. 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.
2. 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.

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами

электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. 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 9.2.

Таблица 9.2 – 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, определяющимися исходя из состояния обучающегося на момент проверки

9.4. 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.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры БИС
протокол № 11 от «14» 12 2020 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. БИС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463
Заведующий обеспечивающей каф. БИС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	К.С. Сарин	Согласовано, 68c81ca0-0954-467a-8d01-f93a0d553669

РАЗРАБОТАНО:

и.о. заведующего кафедрой, каф. БИС	Е.Ю. Костюченко	Разработано, c6235dfe-234a-4234-88f9-e1597aac6463
Старший преподаватель, каф. ТОР	Д.С. Брагин	Разработано, 7089a338-1c26-46ac-932e-dff575c7cff9