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 УР

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

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ

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: **4**
Семестр: **8**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	8 семестр	Всего	Единицы
Лекционные занятия	28	28	часов
Лабораторные занятия	36	36	часов
Самостоятельная работа	44	44	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	144	144	часов
	4	4	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	8

Томск

1. Общие положения

1.1. Цели дисциплины

1. Обучение студентов основам построения, конфигурирования и эксплуатации распределенных автоматизированных систем, использующих беспроводные каналы передачи данных.

2. Ознакомление обучающихся с принципами защиты информации в локальных сетях беспроводной связи, а также с соответствующими механизмами аутентификации абонентов, обеспечения целостности и конфиденциальности передаваемой информации.

1.2. Задачи дисциплины

1. Ознакомление с многообразием протоколов передачи данных в системах беспроводной связи, с их классификацией и историей их развития.

2. Изучение принципов обеспечения целостности и конфиденциальности сообщений, а также доступности сервисов в системах беспроводной связи.

3. Ознакомление с архитектурой беспроводных сетей на физическом и канальном уровнях модели взаимодействия открытых систем (OSI): аппаратное обеспечение, стандарты, протоколы.

4. Изучение методов аутентификации и распределения ключей в системах беспроводной связи, на примере сетей Wi-Fi.

5. Ознакомление с известными практическими атаками на беспроводные сети Wi-Fi и Bluetooth, а также с программно-аппаратными инструментами тестирования беспроводных сетей на проникновение.

6. Ознакомление с корпусом документов, определяющих требования к беспроводным сетям и их компонентам, на примере спецификации Wi-Fi сетей.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль специальности (special hard skills - SHS).

Индекс дисциплины: Б1.О.03.26.

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-9.3. Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям	ОПК-9.3.1. Знает методы контроля функционирования телекоммуникационных систем и сетей, их защищенности от НСД, принципы построения систем обнаружения компьютерных атак, возможные источники и технические каналы утечки информации в телекоммуникационных системах и сетях	Понимает различия между проводными и беспроводными системами связи в части обеспечения их защищённости. Осознаёт принципиальную важность процедуры распределения сессионных и сеансовых ключей, а также способен определять оценивать риски, связанные с её реализацией.
	ОПК-9.3.2. Умеет применять инструментальные средства проведения мониторинга защищенности телекоммуникационных систем и сетей, составлять отчеты по результатам проверок	Умеет воспроизводить основные известные практические атаки на беспроводные локальные сети, используя при этом специализированный инструментарий (в т.ч. скрипты под Kali Linux) и руководствуясь принципами "этичного хакинга". Умеет анализировать и интерпретировать результаты произведённых тестов, формировать на их основе рекомендации по устранению выявленных в системе уязвимостей.
	ОПК-9.3.3. Владеет навыками анализа защищенности телекоммуникационных систем и сетей с использованием сканеров безопасности и средств автоматического реагирования на попытки несанкционированного доступа	Владеет программными инструментами мониторинга сетевого трафика и способен их применять для обнаружения атак типа "отказ в обслуживании" на беспроводные локальные сети. Способен применять программные средства (в т.ч. включённые в дистрибутив Kali Linux) для автоматизированной оценки защищённости беспроводных сетей.

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	Ознакомлен с многообразием и номенклатурой актуальных стандартов и протоколов, применимых в беспроводных сетях связи. Понимает особенности построения сетей "Интернета вещей" на основе Wi-Fi (802.11ah), BlueTooth LE (802.15.4), LoRaWAN в части обеспечения требований по информационной безопасности, а также автономности и мобильности клиентских станций. Знает принципы анализа и оценки защищённости тех или иных беспроводных сетей, основанные на их архитектуре, конфигурации и применяемых в них протоколах.
	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	Умеет оценивать количественные и вероятностные характеристики беспроводных телекоммуникационных сетей (долю повторных пакетов, скорость передачи данных, BER, SNR, задержку и др.), а также делать выводы об их эффективности на основе проведённых оценок. Может использовать штатные механизмы (и протоколы) обеспечения целостности и конфиденциальности информации, циркулирующей в беспроводных локальных сетях. Умеет конфигурировать Wi-Fi сеть с учётом требований как по эффективности передачи данных, так и по их защищённости.
	ОПК-13.3. Владеет навыком оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	Владеет навыками настройки беспроводных локальных корпоративных сетей (WPA-Enterprise), использующих удалённый сервер аутентификации по протоколу RADIUS. Способен интерпретировать и учитывать в ходе настройки требования по безопасности (в соответствии с RFC 4017) к применяемым методам аутентификации в беспроводных сетях.

ОПК-15. Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	ОПК-15.1. Знает методики измерения и оценки параметров в телекоммуникационных системах и сетях и типовые средства для инструментальной оценки уровня защищённости телекоммуникационных систем	Понимает суть характеристик передающего и приёмного оборудования современных сетей беспроводной связи, в частности мощности передатчика, чувствительности приёмника, диаграммы направленности, лучеформирование и другие. Способен извлекать соответствующую информацию, а также информацию о применяемых в сети механизмах безопасности, из заголовков кадров физического уровня.
	ОПК-15.2. Умеет анализировать пропускную способность и предельную нагрузку сети связи, параметры передачи кадров при прохождении по каналам связи, проверять достижимость абонентов сети связи	Может применять программные инструменты (утилит операционной системы, специализированных скриптов) для оценки пропускной способности беспроводных каналов и построения графа связности устройств в локальной сети. Умеет оценивать предельную нагрузку на локальную беспроводную сеть в инфраструктурном режиме, в том числе, в условиях активной атаки типа "отказ в обслуживании".
	ОПК-15.3. Владеет навыками проведения анализа защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях	Способен на практике применять знания о штатных механизмах безопасности, предусмотренных в тех или иных беспроводных системах связи, для выбора их оптимальной конфигурации. Владеет навыками анализа передаваемых в эфир данных с целью определения используемых в сети криптографических протоколов и процедур аутентификации.
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 4 зачетных единиц, 144 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
		8 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	64	64
Лекционные занятия	28	28
Лабораторные занятия	36	36
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	44	44
Подготовка к тестированию	12	12
Подготовка к лабораторной работе, написание отчета	12	12
Написание отчета по лабораторной работе	20	20
Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	144	144
Общая трудоемкость (в з.е.)	4	4

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	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Общие сведения о беспроводных сетях связи	4	-	2	6	ОПК-13
2 Физический и канальный уровни в системах беспроводной связи	4	8	6	18	ОПК-13, ОПК-15
3 Типовые угрозы и механизмы обеспечения безопасности в беспроводных сетях	4	10	8	22	ОПК-13, ОПК-15, ОПК-9.3
4 Методы аутентификации и распределения ключей в беспроводных сетях	8	8	12	28	ОПК-13, ОПК-9.3
5 Требования к защищённости в современных и перспективных системах беспроводной связи	4	4	8	16	ОПК-15, ОПК-9.3
6 Конфигурирование беспроводных локальных сетей, отвечающих требованиям безопасности	4	6	8	18	ОПК-13, ОПК-15
Итого за семестр	28	36	44	108	
Итого	28	36	44	108	

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
8 семестр			
1 Общие сведения о беспроводных сетях связи	История развития беспроводной связи в телефонных и компьютерных сетях. Особенности, преимущества и недостатки систем беспроводной связи. Классификация беспроводных технологий по дальности действия, по топологии, по области действия.	4	ОПК-13
	Итого	4	

2 Физический и канальный уровни в системах беспроводной связи	Пакетная и синхронная передача в радиоэфире. Методы модуляции и их влияние на характеристики радиоканала. Частотное (OFDM, DBA) и статистическое (FHSS, DSSS, CDMA) мультиплексирование. Методы управления доступом к среде, а также предотвращение и отработка коллизий. Стек протоколов в семействе стандартов 802.	4	ОПК-13
	Итого	4	
3 Типовые угрозы и механизмы обеспечения безопасности в беспроводных сетях	Угрозы конфиденциальности и целостности информации в радио канале. Угрозы доступности сервисов беспроводной сети. Криптографическая защита сообщений (шифрование, имитовставки, хеширование). Протоколы для криптографической защиты сообщений (RC4, CCMP, GCMP). Аутентификация и распределение ключей между узлами сети. Иерархия ключей (мастер-ключи, сессионные ключи, сеансовые ключи).	4	ОПК-9.3
	Итого	4	
4 Методы аутентификации и распределения ключей в беспроводных сетях	Взаимная и односторонняя аутентификация. Аутентификация с общим секретом. Аутентификация с "оракулом". Аутентификация в Bluetooth, Wi-Fi (WEP). Аутентификация в Wi-Fi (RSN). Четырёхэтапное рукопожатие в WPA/WPA2. Расширяемый протокол аутентификации EAP. Протокол EAPOL. Протокол быстрого конфигурирования WPS. Практические атаки на аутентификацию (и конфигурирование) в беспроводных сетях.	8	ОПК-9.3
	Итого	8	
5 Требования к защищённости в современных и перспективных системах беспроводной связи	Требования по безопасности к методам аутентификации (RFC 4017). Идеальная прямая защищённость. Словарная атака. Атака Дэннинга-Сако. Применение X.509 сертификатов. Аутентификация с TLS-туннелированием. Криптографическая привязка. Безопасные методы аутентификации на основе EAP-TTLS. Безопасные методы аутентификации с паролем (SPEKE, DH-EKE, SAE).	4	ОПК-9.3
	Итого	4	

6 Конфигурирование беспроводных локальных сетей, отвечающих требованиям безопасности	Спецификация WPA3. Защита служебных кадров (PMF). Режим повышенной безопасности в WPA3. Протокол быстрого конфигурирования DPP. Особенности корпоративных WLAN-сетей (WPA-Enterprise). Протокол RADIUS. Настройка сервера аутентификации и домена.	4	ОПК-13
	Итого	4	
Итого за семестр		28	
Итого		28	

5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

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
8 семестр			
2 Физический и канальный уровни в системах беспроводной связи	Подготовка рабочего места	4	ОПК-15
	Изучение структуры кадров, механизмов взаимного обнаружения и потоков сообщений в Wi-Fi сетях	4	ОПК-15
	Итого	8	
3 Типовые угрозы и механизмы обеспечения безопасности в беспроводных сетях	Исследование и эксплуатация уязвимостей протокола безопасности WEP	6	ОПК-9.3, ОПК-15
	Атаки типа "отказ в обслуживании" с помощью утилиты MDK4	4	ОПК-9.3, ОПК-13, ОПК-15
	Итого	10	
4 Методы аутентификации и распределения ключей в беспроводных сетях	Словарные атаки на персональные беспроводные сети (WPA/WPA2)	4	ОПК-9.3, ОПК-13
	Практические атаки на протокол автоматизированного конфигурирования безопасной сети WPS	4	ОПК-9.3, ОПК-13
	Итого	8	
5 Требования к защищённости в современных и перспективных системах беспроводной связи	Автоматизированный аудит безопасности беспроводных локальных сетей	4	ОПК-9.3, ОПК-15
	Итого	4	

6 Конфигурирование беспроводных локальных сетей, отвечающих требованиям безопасности	Безопасное конфигурирование корпоративной беспроводной сети (WPA-Enterprise)	6	ОПК-13, ОПК-15
	Итого	6	
Итого за семестр		36	
Итого		36	

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
8 семестр				
1 Общие сведения о беспроводных сетях связи	Подготовка к тестированию	2	ОПК-13	Тестирование
	Итого	2		
2 Физический и канальный уровни в системах беспроводной связи	Подготовка к тестированию	2	ОПК-15	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ОПК-15	Лабораторная работа
	Написание отчета по лабораторной работе	2	ОПК-15	Отчет по лабораторной работе
	Итого	6		
3 Типовые угрозы и механизмы обеспечения безопасности в беспроводных сетях	Подготовка к тестированию	2	ОПК-9.3, ОПК-13, ОПК-15	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ОПК-9.3, ОПК-13, ОПК-15	Лабораторная работа
	Написание отчета по лабораторной работе	4	ОПК-9.3, ОПК-13, ОПК-15	Отчет по лабораторной работе
	Итого	8		
4 Методы аутентификации и распределения ключей в беспроводных сетях	Подготовка к тестированию	2	ОПК-9.3, ОПК-13	Тестирование
	Подготовка к лабораторной работе, написание отчета	4	ОПК-9.3, ОПК-13	Лабораторная работа
	Написание отчета по лабораторной работе	6	ОПК-9.3, ОПК-13	Отчет по лабораторной работе
	Итого	12		

5 Требования к защищённости в современных и перспективных системах беспроводной связи	Подготовка к тестированию	2	ОПК-9.3, ОПК-15	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ОПК-9.3, ОПК-15	Лабораторная работа
	Написание отчета по лабораторной работе	4	ОПК-9.3, ОПК-15	Отчет по лабораторной работе
	Итого	8		
6 Конфигурирование беспроводных локальных сетей, отвечающих требованиям безопасности	Подготовка к тестированию	2	ОПК-13, ОПК-15	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ОПК-13, ОПК-15	Лабораторная работа
	Написание отчета по лабораторной работе	4	ОПК-13, ОПК-15	Отчет по лабораторной работе
	Итого	8		
Итого за семестр		44		
	Подготовка и сдача экзамена	36		Экзамен
Итого		80		

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.	Лаб. раб.	Сам. раб.	
ОПК-9.3	+	+	+	Лабораторная работа, Отчет по лабораторной работе, Тестирование, Экзамен
ОПК-13	+	+	+	Лабораторная работа, Отчет по лабораторной работе, Тестирование, Экзамен
ОПК-15		+	+	Лабораторная работа, Отчет по лабораторной работе, 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
8 семестр				
Лабораторная работа	8	8	8	24

Тестирование	4	4	4	12
Отчет по лабораторной работе	6	14	14	34
Экзамен				30
Итого максимум за период	18	26	26	100
Нарастающим итогом	18	44	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. Ковцур, М. М. Безопасность беспроводных сетей / М. М. Ковцур , Д. В. Юркин, Е. Ю. Герлинг, К. А. Ахрамеева — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022. — 71с. — ISBN 978-5-89160-227-4. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/279623.

7.2. Дополнительная литература

1. Кашкаров, А. П. Электронные устройства для глушения беспроводных сигналов (GSM, Wi-Fi, GPS и некоторых радиотелефонов) / А. П. Кашкаров. — Москва : ДМК Пресс, 2016. — 96 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/90125.

2. Чанцис, Ф. Практическии хакинг интернета вещеи / Ф. Чанцис, И. Стаис ; перевод с английского Л. Н. Акулич. — Москва : ДМК Пресс, 2022. — 480 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/241214.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Поздняк, И. С. Базовые настройки безопасности беспроводных сетей 802.11 : методические указания / И. С. Поздняк. — Самара : ПГУТИ, 2020. — 10 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/255563.

2. Поздняк, И. С. Обеспечение безопасности в беспроводных сетях : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 22 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/223310.

3. Макаров, И. С. Проектирование проводных и беспроводных сетей в среде NS2 : методические указания / И. С. Макаров, М. А. Буранова. — Самара : ПГУТИ, 2019. — 16 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/223250.

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 лабораторных работ

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Магнитно-маркерная доска;
- Обучающий стенд локальные компьютерные сети Microtik routerboard - 2 шт.;
- ViPNET УМК "Безопасность сетей";
- Коммутатор Mikrotik CRS125-24G-1S-IN - 6 шт.;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 - 3 шт.;
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 - 2 шт.;

- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 - 2 шт.;
- Маршрутизатор Cisco C881-V-K9 - 2 шт.;
- Маршрутизатор Check Point CPAP-SG1200R-NGFW - 2 шт.;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:
- абонентские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- межсетевые экраны: ИКС Lite, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- точки доступа: D-link dwl3600ap.

Стенды для изучения средств криптографической защиты информации в банковском деле, включающие:
- абонентские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства криптографической защиты информации: программно-аппаратный комплекс шифрования "ФПСУ-IP", программно-аппаратный комплекс шифрования "ФПСУ-IP/Клиент".
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:
- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 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.

8.4. 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 Общие сведения о беспроводных сетях связи	ОПК-13	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
2 Физический и канальный уровни в системах беспроводной связи	ОПК-13, ОПК-15	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
3 Типовые угрозы и механизмы обеспечения безопасности в беспроводных сетях	ОПК-13, ОПК-15, ОПК-9.3	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
4 Методы аутентификации и распределения ключей в беспроводных сетях	ОПК-13, ОПК-9.3	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ

5 Требования к защищённости в современных и перспективных системах беспроводной связи	ОПК-15, ОПК-9.3	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
6 Конфигурирование беспроводных локальных сетей, отвечающих требованиям безопасности	ОПК-13, ОПК-15	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ

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. Какой из перечисленных протоколов используется для шифрования данных:
   a. CCMP.
   b. ICMP.
   c. MIC.
   d. CDMA/CA.
2. Какая из перечисленных спецификацией применяется, преимущественно, в сетях персонального уровня:
   a. 802.15 (Wi-Fi).
   b. 802.11 (BlueTooth).
   c. 802.16 (WiMAX).
   d. 802.15 (BlueTooth).
3. Какой из перечисленных методов аутентификации с паролем подвержен офлайн словарной атаке:
   a. WPA-PSK (Wi-Fi).
   b. Простое сопряжение (BlueTooth).
   c. WPA-SAE (Wi-Fi).
   d. PKI-аутентификация (WiMAX).
4. Какой из перечисленных принципов не относится к "этическому хакингу" …
   a. Взаимодействие с системой должно быть авторизированным её владельцем.
   b. Все заинтересованные стороны (пользователи, регуляторы, владелец, разработчик и пр.) должны быть уведомлены о факте проверке и об её итогах.
   c. Все выявленные уязвимости и последствия их эксплуатации должны быть доведены до заказчика.
   d. Относятся все.
5. Какой из перечисленных приёмов является достаточным для обеспечения целостности пакетов данных передаваемых в эфир:
   a. Контрольная сумма.
   b. Имитовставка.
   c. Шифрование.
   d. Хеширование.
6. Сколько уровней содержит модель взаимодействия открытых систем (OSI) ?

a. 3.
b. 7.
c. 5.
d. 4.

7. Какой уровень модели взаимодействия открытых систем занимает подуровень MAC:
   a. сетевой.
   b. физический.
   c. канальный.
   d. канальный и физический.
8. 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.
9. Какую функцию в Wi-Fi сетях выполняет механизм CSMA/CA:
   a. Защиту конфиденциальности данных.
   b. Адаптивный выбор канала коммуникации.
   c. Генерацию уникальных ключей.
   d. Предотвращение коллизий.
10. Протокол RADIUS используется для…
    a. Определения границ охвата беспроводной сети.
    b. Взаимодействия аутентификатора с сервером аутентификации.
    c. Автоматическую настройку энергетических параметров приёмопередатчиков.
    d. Взаимодействия аутентифицируемого с аутентификатором.
11. Какой из принципов не закладывался при проектировании WEP:
    a. Обязательность применения для защиты конфиденциальности данных.
    b. Получение экспортного разрешения от американского регулятора.
    c. "Достаточная" защищённость, адекватная для применения в личных сетях.
    d. Ни один из названных.
12. Какая практическая атака на WEP не направлена на получении ключа?
    a. Атака FMS/KoreK.
    b. Атака по частям (Chop-Chop).
    c. Атака PTW.
    d. Атака KRACK.
13. Какое из перечисленных беспроводных решений не предназначено для применения в приложениях "Интернета вещей":
    a. Wi-Fi HaLow (802.11ah)
    b. BlueTooth LE (802.15.4).
    c. LoRaWAN.
    d. Mobile WiMAX (802.16m).
14. Какая из характеристик не применима к аутентификации в WEP с общим секретом:
    a. Однонаправленность.
    b. Распределение парного сессионного ключа.
    c. Использование секрета с энтропией 40 бит или 104 бита.
    d. Высокий риск компрометации ключевого потока.
15. Какой из ключей находится выше в иерархии Wi-Fi сетей (не может быть тривиально получен из других):
    a. Сессионный мастер-ключ (MSK).
    b. Парный мастер-ключ (PMK).
    c. Парный сеансовый ключ (PTK).
    d. Ключ шифрования ключей (KEK).
16. Какой из перечисленных инструментов предназначен для тестирования на уязвимости локальных беспроводных сетей
    a. aircrack-ng.
    b. WiFisher.
    c. Crunch.
    d. WireShark.

17. Что означает уязвимость протокола аутентификации с паролем к атаке Деннинга-Сакко?
    a. Пароль может быть получен путём офлайн атаки со словарём.
    b. Компрометация пароля скомпрометирует данные, перехваченные в ходе предыдущих сеансов.
    c. Компрометация сгенерированного сеансового ключа может привести к компрометации пароля или будущих сеансовых ключей.
    d. Атака не имеет отношения к процедуре аутентификации.
18. 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.
19. Какая из перечисленных беспроводных технологий не относится к классу WPAN?
    a. ZigBee.
    b. Bluetooth.
    c. UWB.
    d. UMTS.
20. "Абсолютная прямая защищённость" протокола аутентификации с паролем означает:
    a. Невозможность словарной офлайн атаки.
    b. То, что безопасность аутентификации гарантируется только в одном направлении (в отношении клиента).
    c. То, что компрометация пароля в будущем не скомпрометирует данные, перехваченные в ходе предыдущих сеансов.
    d. Использование туннелирования для защиты от атаки типа "человек посередине".
21. В каком протоколе аутентификации не используется криптографическая схема Диффи-Хеллмана:
    a. SAE (Wi-Fi WPA-Personal).
    b. EAP-TLS (Wi-Fi WPA-Enterprise).
    c. Простое сопряжение (BlueTooth).
    d. Во всех перечисленных.
22. Какие преимущества протокола экспоненциального обмена ключами с паролем (SPEKE) имеют место по сравнению с протоколом аутентификации с косвенным согласованием (CHAP):
    a. Устойчивость к словарным офлайн атакам.
    b. Абсолютная прямая защищённость.
    c. Подходит для генерации сеансовых ключей.
    d. Все перечисленные.
23. Криптография необходима для реализации следующих сервисов безопасности:
    a. Контроль конфиденциальности.
    b. Контроль вторжений.
    c. Контроль доступности.
    d. Контроль непротиворечивости.
    Ответ____
24. Какое из утверждений об атаке Pixie Dust несправедливо:
    a. Направлена против Wi-Fi сетей с поддержкой WPS.
    b. Эксплуатирует уязвимость с генерацией секретной соли.
    c. Требует многократных попыток выполнения протокола конфигурации (взаимодействия с точкой доступа).
    d. Позволяет получить кодовую фразу (применительно к персональным сетям).
25. Какой из протоколов пришёл на смену WPS:
    a. TKIP (Temporal Key Integrity Protocol).
    b. GCMP (Galois Counter Mode Protocol).
    c. DPP (Device Provisioning Protocol).

d. CDMA (Code Division Multiple Access).

26. Какие из перечисленных MAC кадров не относятся к классу служебных (management):
    a. Маячки (beacons).
    b. Подтверждения получения (acknowledgements).
    c. Зондирующие запросы (probe requests).
    d. Запросы деаутентификации.
27. Какая из характеристик не применима к аутентификации в WPA-PSK:
    a. Однонаправленность.
    b. Высокий риск компрометации ключевого потока.
    c. Использование секрета с энтропией 40 бит или 104 бита.
    d. Ни одна из перечисленных.
28. Какой режим применения блочного шифра AES-128 не применяется в CCMP:
    a. Сцепление блоков шифротекста (CBC).
    b. Электронная кодовая книга (ECB).
    c. Счётчик (CTR).
    d. Применяются все.
29. Преимущество GCMP перед CCMP состоит в...
    a. В устранении уязвимости повторного использования значения в счётчике кадров.
    b. Лучшей криптостойкости шифра.
    c. Меньшей вычислительной сложности и большем параллелизме.
    d. Меньшей длине имитовставки.
30. Какая из атак типа "отказ в обслуживании" не реализована в MDK4:
    a. Атака деаутентификации/деассоициации.
    b. Атака аутентификации.
    c. Атака авторизации.
    d. Все реализованы.

9.1.2. Перечень экзаменационных вопросов

1. Способы модуляции в беспроводных сетях (GFSK, BPSK, QPSK, QAM).
2. Беспроводные сети WPAN (особенности, функции, механизмы безопасности).
3. Беспроводные сети WMAN (особенности, функции, механизмы безопасности).
4. Оборудование WLAN сетей (адаптеры, точки доступы, повторители, мосты).
5. Стек протоколов WLAN (функции подуровней).
6. Управление доступом к среде в WLAN (функции координации, CSMA/CA, RTS/CTS).
7. Типы MAC-кадров в WLAN (функции, особенности заголовков).
8. Взаимное обнаружение устройств в WLAN. Функции и содержание элемента RSN IE.
9. Аутентификация (преаутентификация) и ассоциация.
10. Подтипы служебных кадров (management frames) и их функции.
11. Сервисы в WLAN. BSS и ESS. Управление сервисом (QoS). Механизм быстрого перехода (Fast transition).
12. Документы спецификации IEEE 802.11 (терминология, содержание, именование).
13. Wi-Fi Alliance. Регламентирующие документы Wi-Fi Alliance (роль, содержание).
14. Архитектура безопасности в WLAN (функции безопасности в RSN-сетях).
15. Понятие криптографического набора (cypher suite). Защита однонаправленного и широковещательного трафика. Виды криптографических наборов.
16. Понятия WPA/WPA2, WPA3, WPA-Enterprise, WPA-Personal. Маркировка Wi-Fi Certified.
17. Протокол безопасности WEP (конфиденциальность и целостность).
18. Аутентификация в WEP (открытая и с ключом). Соображения безопасности.
19. Уязвимости WEP. Практические атаки на WEP.
20. Обобщённая процедура установления защищённого подключения в сетях RSN.
21. Иерархия ключей в RSN сетях (MSK, PSK, PMK, GTK, KCK и др.).
22. Четырёхэтапное рукопожатие.
23. Протокол TKIP (функции, архитектура, известные уязвимости).
24. Протокол CCMP (функции, архитектура, известные уязвимости).
25. Словарная атака на WPA-Personal (механизм, соображения безопасности).
26. Соображения безопасности при аутентификации с общим ключом (применительно к WPA/WPA2, применительно к WPA3).

27. Спецификация Wi-Fi Protected Setup (назначение, особенности, безопасность).
28. Практические атаки на WPS.
29. Требования к EAP-методам (RFC 4017).
30. EAP-методы с паролем (MD5, MSCHAPv2, EHASH).
31. Метод EAP-TLS.
32. EAP-методы с туннелированием (TTLS, PEAP, FAST).
33. Атаки типа «отказ в обслуживании» в WLAN.
34. Спецификация WPA3 (основные нововведения).
35. Протокол GCMP (функции, архитектура, известные уязвимости).
36. Защита служебных кадров (PMF). Механизм защиты запросов повторной ассоциации.
37. Понятие и назначение эквивалентного уровня безопасности в WPA3 (128 бит, 192 бита).
38. Совместная выработка ключа (с паролем). Протокол SPEKE.
39. Рукопожатие SAE.
40. Спецификация Wi-Fi Easy Connect (назначение, особенности, безопасность).
41. Протокол DPP. Роли и фазы. Бутстрэппинг.
42. Аутентификация в DPP.
43. Kali Linux. Инструменты тестирования безопасности (aircrack, MDK4, WiFite, др.).
44. Беспроводные технологии в приложениях Интернета вещей (протоколы, применение).
45. Протокол LoRaWAN (назначение, особенности, безопасность).
46. Типовая архитектура системы Интернета вещей. Соображения безопасности.

9.1.3. Темы лабораторных работ

1. Подготовка рабочего места
2. Изучение структуры кадров, механизмов взаимного обнаружения и потоков сообщений в Wi-Fi сетях
3. Исследование и эксплуатация уязвимостей протокола безопасности WEP
4. Атаки типа "отказ в обслуживании" с помощью утилиты MDK4
5. Словарные атаки на персональные беспроводные сети (WPA/WPA2)
6. Практические атаки на протокол автоматизированного конфигурирования безопасной сети WPS
7. Автоматизированный аудит безопасности беспроводных локальных сетей
8. Безопасное конфигурирование корпоративной беспроводной сети (WPA-Enterprise)

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 9.4.

Таблица 9.4 – 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 № 1 от «24» 1 2023 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
И.О. начальника учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	А.Ю. Якимук	Согласовано, 4ffdf265-fb78-4863-b293-f03438cb07cc

РАЗРАБОТАНО:

Профессор, каф. КИБЭВС	В.С. Аврамчук	Разработано, 20931903-6ee4-4022-abd3-9fb51bd845ca
Старший преподаватель, каф. КИБЭВС	В.А. Фаерман	Разработано, 7e6b5d61-ea75-4d93-80c5-464a05c34921