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
Сенченко П.В.
«18» 02 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Уровень образования: высшее образование - магистратура

Направление подготовки / специальность: 10.04.01 Информационная безопасность

Направленность (профиль) / специализация: Информационная безопасность объектов

критической информационной инфраструктуры

Форма обучения: очная

Факультет: Факультет безопасности (ФБ)

Кафедра: Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

Курс: **2** Семестр: **3**

Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	3 семестр	Всего	Единицы
Лекционные занятия	36	36	часов
Практические занятия	36	36	часов
Лабораторные занятия	8	8	часов
Курсовая работа	36	36	часов
Самостоятельная работа	64	64	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость	216	216	часов
(включая промежуточную аттестацию)	6	6	3.e.

Формы промежуточной аттестация	Семестр
Экзамен	3
Курсовая работа	3

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Сенченко П.В.

Должность: Проректор по УР Дата подписания: 18.02.2022 Уникальный программный ключ: a1119608-cdff-4455-b54e-5235117c185c

1. Общие положения

1.1. Цели дисциплины

- 1. Освоение дисциплинарных компетенций, связанных с созданием и изучением современной защищенных информационных систем различного применения и степени сложности.
- 2. Обучение принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных информационных систем, а также содействовать формированию научного мировоззрения и развитию системного мышления.

1.2. Задачи дисциплины

- 1. Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности.
- 2. Обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.
- 3. Разработка систем, комплексов, средств и технологий обеспечения информационной безопасности.
- 4. Разработка программ и методик испытаний средств и систем обеспечения информационной безопасности.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули). Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль направления подготовки (hard skills – HS).

Индекс дисциплины: Б1.О.2.4.

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

индикаторы достижения Планируемые результаты обучения				
Компетенция	компетенции	дисциплине		
Универсальные компетенции				
Общепрофессиональные компетенции				

ОПК-1. Способен	ОПК-1.1. Знает меры	Знает принципы разработки защищенных
обосновывать требования к		информационных систем различного применения
системе обеспечения	и технологии обеспечения	и степени сложности.
информационной	информационной безопасности	
безопасности и	ОПК-1.2. Знает уязвимости	Знает методики выявления угроз и оценки
разрабатывать проект	систем и угрозы	уязвимостей информационных систем.
технического задания на ее	информационной безопасности	
создание;	ОПК-1.3. Знает нормативную	Знает методы и средства обеспечения
	базу и ГОСТы,	информационной безопасности, а также
	регламентирующие процесс	нормативную базу регламентирующую
	разработки технических заданий	классификацию данных средств.
	на создание систем обеспечения	
	информационной безопасности	
	объектов	
	ОПК-1.4. Умеет обосновывать	Умеет обосновывать требования к процессам и
	требования к процессам и	технологиям обеспечения информационной
	технологиям обеспечения	безопасности объектов критической
	информационной безопасности	информационной инфраструктуры.
	ОПК-1.5. Умеет осуществлять	Умеет осуществлять выбор подсистем,
	выбор подсистем, реализующих	реализующих технологии обеспечения
	технологии обеспечения	информационной безопасности для объектов
	информационной безопасности	критической информационной инфраструктуры.
	ОПК-1.6. Умеет обосновывать	Умеет обосновывать требования к мерам
	требования к мерам обеспечения	обеспечения информационной безопасности
	информационной безопасности	объектов критической информационной
		инфраструктуры.
	ОПК-1.7. Умеет разрабатывать	Умеет составлять техническое задание по
	техническое задание на создание	разработке систем, комплексов, средств и
	подсистемы обеспечения	технологий обеспечения информационной
	информационной безопасности	безопасности.
	ОПК-1.8. Знает отечественные и	Знает как обосновывать выбор состава,
	зарубежные стандарты в области	характеристик и функциональных возможностей
	обеспечения информационной	систем и средств обеспечения информационной
	безопасности	безопасности объектов защиты на основе
		российских и международных стандартов.
	ОПК-1.9. Знает нормативную и	Знает основные нормативные методические
	правовую базу в области	документы ФСБ России, ФСТЭК России,
	обеспечения информационной	касающиеся разработки средств защиты
	безопасности, нормативные	информации
	методические документы ФСБ	
	России, ФСТЭК России и иных	
	регуляторов в области	
	обеспечения информационной	
	безопасности	
	ОПК-1.10. Знает основы	Знает типовые требования к разработке средств
	управления рисками	защиты, направленные на снижение рисков
	информационной безопасности	информационной безопасности.
	ОПК-1.11. Умеет оценивать	Умеет настраивать средства защиты информации
	риски информационной	в соответствии с требованиями к объекту защиты
	безопасности	с целью снижения рисков информационной
		безопасности.

ОПК-2. Способен	ОПК-2.1. Знает принципы	Знает принципы организации и этапы разработки
разрабатывать	организации и этапы разработки	системы (подсистемы либо компонента системы)
технический проект	системы (подсистемы либо	обеспечения информационной безопасности
системы (подсистемы либо	компонента системы)	объектов критической информационной
компонента системы)	обеспечения информационной	инфраструктуры.
обеспечения	безопасности	
информационной	ОПК-2.2. Знает средства	Знает методики испытаний средств и систем
безопасности;	тестирования системы	обеспечения информационной безопасности
	(подсистемы либо компонента	
	системы) обеспечения	
	информационной безопасности	
	ОПК-2.3. Умеет разрабатывать	Умеет составлять требования и критерии оценки
	модели угроз и нарушителей	информационной безопасности.
	информационной безопасности	T of
	ОПК-2.4. Умеет разрабатывать	Умеет разрабатывать программы и методики
	планы и сценарии тестирования	испытаний средств и систем обеспечения
	системы (подсистемы либо	информационной безопасности объектов
	компонента системы)	критической информационной инфраструктуры.
	обеспечения информационной	
	безопасности	
	ОПК-2.5. Умеет разрабатывать	Умеет разрабатывать требования к средствам и
	требования к средствам и	методам контроля проектируемой системы
	методам контроля	(подсистемы либо компонента системы)
	проектируемой системы	обеспечения информационной безопасности
	(подсистемы либо компонента	объектов критической информационной
	системы) обеспечения	инфраструктуры.
	информационной безопасности	
	ОПК-2.6. Умеет разрабатывать и	Умеет разрабатывать и реализовывать
	реализовывать технический	технический проект системы (подсистемы либо
	проект системы (подсистемы	компонента системы) обеспечения
	либо компонента системы)	информационной безопасности объектов
	обеспечения информационной	критической информационной инфраструктуры.
	безопасности	
	Профессиональные к	сомпетенции
-	-	-
	1	1

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

Two man in This was a second and a second an	-	1
Виды учебной деятельности		Семестры
Виды учесной деятельности	часов	3 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	116	116
Лекционные занятия	36	36
Практические занятия	36	36
Лабораторные занятия	8	8
Курсовая работа	36	36
Самостоятельная работа обучающихся, в т.ч. контактная	64	64
внеаудиторная работа обучающихся с преподавателем, всего		
Написание отчета по курсовой работе	36	36
Подготовка к тестированию	6	6

Написание отчета по практическому занятию (семинару)	18	18
Подготовка к лабораторной работе, написание отчета	4	4
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

Гаолица 5.1 – Разделы (темы) дисциплины и виды учеоной деятельности							
Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Лаб. раб.	Курс. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
		3 ce	местр				
1 Теоретические вопросы защиты информации и построения информационных систем	8	8	-	36	9	61	ОПК-1, ОПК-2
2 Проектирование автоматизированных информационных систем	4	8	-		13	25	ОПК-1, ОПК-2
3 Содержание работ на этапах создания автоматизированных информационных систем	8	12	-		15	35	ОПК-1, ОПК-2
4 Способы и методы защиты информации в информационных системах	10	8	-		14	32	ОПК-1, ОПК-2
5 Средства разработки и тестирования автоматизированных информационных систем	6	-	8		13	27	ОПК-1, ОПК-2
Итого за семестр	36	36	8	36	64	180	
Итого	36	36	8	36	64	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
	3 семестр		

1 Теоретические	Автоматизированная информационная	4	ОПК-1, ОПК-2
вопросы защиты	система. Классификации задач, решаемых		
информации и	с использованием информационных		
построения	систем. Свойства систем. Классификации		
информационных	систем. Ранги систем. Закон		
систем	необходимости разнообразия (закон		
	Эшби).		
	Основы теории надежности. Связь с	2	ОПК-1, ОПК-2
	основными задачами информационной		
	без-опасности. Надежность программно-		
	аппаратных реализаций информационных		
	систем.		
	Подходы к проектированию и реализации информационных систем. Жизненный	2	ОПК-1, ОПК-2
	цикл информационной системы. Вопросы		
	информационной безопасности и аспекты		
	построения защищенных систем. Место		
	процесса кодирования и языка		
	программирования в проблемах		
	информационной безопасности		
	Итого	8	
2 Проектирование	Изучение государственных стандартов,	4	ОПК-1, ОПК-2
автоматизированных	содержащих требования, устанавливаемые		
информационных	российским законодательством к		
систем	построению автоматизированных систем-		
	ГОСТ 24.104-85 «Автоматизированные		
	системы управления. Общие требования.		
	Единая система стандартов» и ГОСТ		
	34.003- 90«Информационная технология.		
	Комплекс стандартов на		
	автоматизированные системы. Термины и		
	определения». Изучение специфики		
	научно-исследовательской работы		
	Итого	4	

3 Содержание работ	Изучение государственных стандартов,	4	ОПК-1, ОПК-2
на этапах создания	содержащих требования, устанавливаемые		
автоматизированных	российским законодательством к стадиям		
информационных	создания автоматизированных систем -		
систем	ГОСТ 19.102-77 «ЕСПД Стадии		
	разработки», ГОСТ 24.601-86		
	«Автоматизированные системы. Стадии		
	создания», ГОСТ 24.602-86		
	«Автоматизированные системы		
	управления. Со-став и содержание работ		
	по стадиям создания» и ГОСТ34.601-90		
	«Информационная технология. Комплекс		
	стандартов на автоматизированные		
	системы. Автоматизированные системы.		
	Стадии создания». Рассмотрение вопроса		
	разбиения проекта на этапы и определения		
	ключевых параметров каждого из них.		
	Рассмотрение методики построения IDEF.		
	Изучение государственных стандартов,	4	ОПК-1, ОПК-2
	содержащих требования, устанавливаемые		, -
	российским законодательством к		
	оформлению документации по этапам		
	разработки –ГОСТ 19.101-77 (СТ СЭВ		
	1626- 79)«ЕСПД Виды программ и		
	программных документов» и		
	ГОСТ34.201-89 «Информационная		
	технология. Комплекс стандартов на		
	автоматизированные системы. Виды,		
	комплектность и обозначение документов		
	при создании автоматизированных		
	систем». Ознакомление с ГОСТ		
	РИСО/МЭК15408-1-2008		
	«Информационная технология. Методы и		
	средства обеспечения безопасности.		
	Критерии оценки безопасности		
	информационных технологий. Часть 1.		
	Введение и общая модель». Рассмотрение		
	типового комплекта документации		
	Итого	8	

4 Способы и методы	Типология распределенных	4	ОПК-1, ОПК-2
защиты информации	информационных систем. Процессы в		
в информационных	информационных системах. Тенденции и		
системах	подходы к защите информации в		
	информационных системах.		
	Методы и способы обеспечения	2	ОПК-1, ОПК-2
	идентификации, аутентификации и		
	авторизации в информационных системах.		
	Криптографическая защита информации.		
	Понятие несанкционированного доступа и		
	принципы защиты от		
	несанкционированного доступа.		
	Мониторинг и аудит в информационных		
	системах.		
	Стандарты и нормативные документы в	4	ОПК-1, ОПК-2
	области информационной безопасности.		
	Построение защищенной информационной		
	системы в соответствии с нормативами и		
	требованиями. Защита информационных		
	систем, обрабатывающих персональные		
	данные. Государственные		
	информационные системы. Системы		
	управления технологическими		
	процессами. Подходы к аудиту и оценке		
	защищенности информационных систем		
	Итого	10	

	1++		0774.4.0774.4
5 Средства	Изучение государственных стандартов,	4	ОПК-1, ОПК-2
разработки и	содержащих требования, устанавливаемые		
тестирования	российским законодательством к		
автоматизированных	построению модуля безопасности - ГОСТ		
информационных	Р50739- 95 «Средства вычисли-тельной		
систем	техники. Защита от несанкционированного		
	доступа к информации. Общие		
	технические требования», ГОСТ Р		
	34.10-2001 «Информационная техно-логия.		
	Криптографическая защита ин-формации»		
	и ГОСТ Р ИСО/МЭК 15408-2-2008		
	«Информационная технология. Методы и		
	средства обеспечения без-опасности.		
	Критерии оценки безопасности		
	информационных технологий. Часть 2.		
	Функциональные требования без-		
	опасности». Ознакомление с содержанием		
	ГОСТ Р ИСО/МЭК 154О8-3-2008		
	«Информационная технология. Методы и		
	средства обеспечения Безопасности.		
	Критерии оценки Безопасности		
	информационных технологий. Часть 3.		
	Требования доверия к безопасности Условные обозначения». Изучение		
	технологии за-боты ядра безопасности,		
	мониторов об-ращений и прочих		
	компонентов, позволяющих обеспечить		
	безопасность создаваемого программного		
	комплекса. Рассмотрение примеров		
	документации. Рассмотрение типовых		
	профилей защиты автоматизированных		
	систем.		
	Изучение государственного стандарта,	2	ОПК-1, ОПК-2
	содержащего требования,	2	OHK-1, OHK-2
	устанавливаемые российским		
	законодательством к тестированию		
	автоматизированных систем - ГОСТ		
	34.603-92 «Информационная технология.		
	Виды испытаний автоматизированных		
	систем». Изучение видов испытаний и		
	технологию их приме-нения на практике.		
	Рассмотрение примеров документации		
	Итого	6	
	Итого за семестр	36	
	*	36	
	Итого	30	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3. Таблица 5.3. – Наименование практических занятий (семинаров)

Названия разделов (тем)	Наименование практических занятий	Трудоемкость,	Формируемые
дисциплины	(семинаров)	Ч	компетенции

	3 семестр		
1 Теоретические вопросы защиты информации и построения	Разработка технического задания на защищенную информационную систему	8	ОПК-1, ОПК-2
информационных систем	Итого	8	
2 Проектирование автоматизированных информационных систем	Анализ сертифицированного СЗИ на предмет его функциональных возможностей. Построение модели типа «черный ящик» для исследуемой системы с последующей детализацией по технологии IDEF0.	8	ОПК-1, ОПК-2
	Итого	8	
3 Содержание работ на этапах создания автоматизированных информационных систем	Анализ СЗИ с использованием ГОСТ Р ИСО/МЭК 15408-3-2008«Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения» на предмет оценочных уровней доверия.	12	ОПК-1, ОПК-2
	Итого	12	
4 Способы и методы защиты информационных	Обеспечение информационной безопасности в информационных системах	8	ОПК-1, ОПК-2
системах	Итого	8	
	Итого за семестр	36	
	Итого	36	

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4. Таблица 5.4 — Наименование лабораторных работ

, and the second			_
Названия разделов (тем)	Наименование лабораторных	Трудоемкость,	Формируемые
дисциплины	работ	Ч	компетенции
	3 семестр		
5 Средства разработки и	Проектирование	8	ОПК-1, ОПК-2
тестирования	автоматизированной системы с		
автоматизированных	учетом государственных		
информационных систем	стандартов. Анализ реализации		
	модулей автоматизированных		
	систем.		
	Итого	8	
	8		
	Итого	8	

5.5. Курсовая работа

Содержание, трудоемкость контактной аудиторной работы и формируемые компетенции в

рамках выполнения курсовой работы представлены в таблице 5.5.

Таблица 5.5 – Содержание контактной аудиторной работы и ее трудоемкость

Содержание контактной аудиторной работы	Трудоемкость, ч	Формируемые компетенции
3 семестр		
Проектирование, разработка и обеспечение	18	ОПК-1, ОПК-2
информационной безопасности информационной		
системы.		
Консультации с преподавателем по ходу выполнения	14	ОПК-1, ОПК-2
работы.		
Представление предлагаемого для реализации проекта	4	ОПК-1, ОПК-2
системы.		
Итого за семестр	36	
Итого	36	

Примерная тематика курсовых работ:

- 1. web-ориентированная информационная система;
- 2. информационная система персональных данных;
- 3. персональная информационная система;
- 4. корпоративная информационная система;
- 5. медицинская информационная система.

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

	i			
Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
	3 (семестр		
1 Теоретические вопросы защиты информации и	Написание отчета по курсовой работе	4	ОПК-1, ОПК-2	Курсовая работа, Отчет по курсовой работе
построения информационных	Подготовка к тестированию	1	ОПК-1, ОПК-2	Тестирование
систем	Написание отчета по практическому занятию (семинару)	4	ОПК-1, ОПК-2	Отчет по практическому занятию (семинару)
	Итого	9		
2 Проектирование автоматизированных информационных	Написание отчета по курсовой работе	8	ОПК-1, ОПК-2	Курсовая работа, Отчет по курсовой работе
систем	Подготовка к тестированию	1	ОПК-1, ОПК-2	Тестирование
	Написание отчета по практическому занятию (семинару)	4	ОПК-1, ОПК-2	Отчет по практическому занятию (семинару)
	Итого	13		

				<u> </u>
3 Содержание работ на	Написание отчета по	8	ОПК-1, ОПК-2	Курсовая работа,
этапах создания	курсовой работе			Отчет по
автоматизированных				курсовой работе
информационных	Подготовка к	1	ОПК-1, ОПК-2	Тестирование
систем	тестированию			
	Написание отчета по	6	ОПК-1, ОПК-2	Отчет по
	практическому			практическому
	занятию (семинару)			занятию
				(семинару)
	Итого	15		
4 Способы и методы	Написание отчета по	8	ОПК-1, ОПК-2	Курсовая работа,
защиты информации в	курсовой работе			Отчет по
информационных				курсовой работе
системах	Подготовка к	2	ОПК-1, ОПК-2	Тестирование
	тестированию			
	Написание отчета по	4	ОПК-1, ОПК-2	Отчет по
	практическому			практическому
	занятию (семинару)			занятию
				(семинару)
	Итого	14		
5 Средства разработки	Написание отчета по	8	ОПК-1, ОПК-2	Курсовая работа,
и тестирования	курсовой работе			Отчет по
автоматизированных				курсовой работе
информационных	Подготовка к	1	ОПК-1, ОПК-2	Тестирование
систем	тестированию			
	Подготовка к	4	ОПК-1, ОПК-2	Лабораторная
	лабораторной			работа
	работе, написание			
	отчета			
	Итого	13		
	Итого за семестр	64		
	Подготовка и сдача	36		Экзамен
	экзамена			
	Итого	100		

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

Фотитурина	Виды учебной деятельности					
Формируемые	Лек.	Прак.	Лаб.	Курс.	Сам.	Формы контроля
компетенции	зан.	зан.	раб.	раб.	раб.	
ОПК-1	+	+	+	+	+	Курсовая работа, Лабораторная работа,
						Отчет по курсовой работе, Отчет по
						практическому занятию (семинару),
						Тестирование, Экзамен

ОПК-2	+	+	+	+	+	Курсовая работа, Лабораторная работа,
						Отчет по курсовой работе, Отчет по
						практическому занятию (семинару),
						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
	3	семестр		
Лабораторная работа	0	0	10	10
Тестирование	0	0	20	20
Отчет по практическому занятию (семинару)	20	20	0	40
Экзамен				30
Итого максимум за период	20	20	30	100
Нарастающим итогом	20	40	70	100

Балльные оценки для курсовой работы представлены в таблице 6.1.1.

Таблица 6.1.1 – Балльные оценки для курсовой работы

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		
3 семестр						
Отчет по курсовой работе	35	35	30	100		
Итого максимум за период	35	35	30	100		
Нарастающим итогом	35	70	100	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	А (онрипто)
4 (хорошо) (зачтено)	85 – 89	В (очень хорошо)
	75 – 84	С (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	Е (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва: Горячая линия-Телеком, 2011. — 558 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111016.

7.2. Дополнительная литература

- 1. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. 4-е изд., стер. М. : Академия, 2009. 336 с. (наличие в библиотеке ТУСУР 21 экз.).
- 2. ГОСТ Р ИСО/МЭК 27006-2020. Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности [Электронный ресурс]: Режим доступа: https://protect.gost.ru/document1.aspx?control=31&id=238756.
- 3. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27013-2014 "Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 16 сентября 2014 г. N 1084-ст) [Электронный ресурс]: Режим доступа: https://base.garant.ru/71163006/.
- 4. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27033-3-2014 "Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 9 сентября 2014 г. N 1029-ст) [Электронный ресурс]: Режим доступа: https://base.garant.ru/71163008/.
- 5. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27034-1-2014 "Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 11 июня 2014 г. N 564-ст) [Электронный ресурс]: Режим доступа: https://base.garant.ru/400840227/.
- 6. ГОСТ Р ИСО/МЭК 27038-2016. Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования. [Электронный ресурс]: Режим доступа: https://protect.gost.ru/document1.aspx?control=31&id=204467.
- 7. Национальный стандарт РФ ГОСТ Р 52863-2007 "Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. N 515-ст) [Электронный ресурс]: Режим доступа: https://base.garant.ru/5922958/.
- 8. Национальный стандарт РФ ГОСТ Р 50922-2006 "Защита информации Основные термины и определения" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст) [Электронный ресурс]: Режим доступа: https://base.garant.ru/193664/.

9. Национальный стандарт РФ ГОСТ Р 58412-2019 "Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 21 мая 2019 г. N 204-ст) [Электронный ресурс]: — Режим доступа: https://base.garant.ru/72370492/.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Конев, А. А. Защищенные информационные системы: учебно-методическое пособие [Электронный ресурс] / А. А. Конев, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 60 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9990.

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

Лаборатория защищенных автоматизированных систем: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 511 ауд.

Описание имеющегося оборудования:

- Профессиональный компьютерный полиграф "Диана-04+";
- Стенд "Средства контроля и управления доступом" в составе:
- сетевой контроллер СКУД Gate-4000 UPS;
- контроллер управления доступом UnitECO LOCK 2S-LO-SMB;
- турникет PERCo-KT03/600-1;
- источник вторичного электропитания СКАТ-1200М;
- контроллер замка PERCo-CL05;
- контрольный считыватель для карт PERCo-IR05;
- электромагнитный замок ML-295K.

- Стенд "Монтажный стол" в составе:
- паяльная станция Quick 936BESD;
- шкаф для комплектующих ШДК-45С;
- набор монтажных инструментов.
- Стенд "Программно-аппаратный комплекс лифтового хозяйства";
- Стенд "Рабочее место оператора видеонаблюдения" в составе:
- приемопередатчики видеосигнала по витой паре на TTP111VLH;
- видеосервер Domination D7-8-H264;
- видеорегистратор Videorox DVR VR 3294;
- стандартная цветная видеокамера под объектив MSC-512S;
- купольная видеокамера SCW-422;
- пульт управления камерами SPEED DOME SCJ-200;
- видео камера сетевая SPEED DOME Beward BD75-5;
- уличная видеокамера SPEED.
- Стенд "Системы видеонаблюдения" в составе:
- видеорегистратор DHI-NVR4216-16P-4KS2;
- источник бесперебойного питания UPS 400VA Ippon Back.
- Стенд "Пожарно-охранные сигнализации" в составе:
- охранное устройство Мираж-GSMA4-03;
- ИК извещатель "РАПИД";
- ИК извещатель "ФОТОН";
- Извещатель радиоволновый Астра-552;
- Комбинированный извещатель Астра-8;
- Извещатель ИПД-3.1М;
- Климатическая станция Vantage PRO2.
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория защищенных автоматизированных систем: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 511 ауд.

Описание имеющегося оборудования:

- Профессиональный компьютерный полиграф "Диана-04+";
- Стенд "Средства контроля и управления доступом" в составе:
- сетевой контроллер СКУД Gate-4000 UPS;
- контроллер управления доступом UnitECO LOCK 2S-LO-SMB;
- турникет PERCo-KT03/600-1;
- источник вторичного электропитания СКАТ-1200М;
- контроллер замка PERCo-CL05;
- контрольный считыватель для карт PERCo-IR05;
- электромагнитный замок ML-295K.
- Стенд "Монтажный стол" в составе:
- паяльная станция Quick 936BESD;
- шкаф для комплектующих ШДК-45С;
- набор монтажных инструментов.
- Стенд "Программно-аппаратный комплекс лифтового хозяйства";
- Стенд "Рабочее место оператора видеонаблюдения" в составе:
- приемопередатчики видеосигнала по витой паре на TTP111VLH;
- видеосервер Domination D7-8-H264;
- видеорегистратор Videorox DVR VR 3294;
- стандартная цветная видеокамера под объектив MSC-512S;
- купольная видеокамера SCW-422;
- пульт управления камерами SPEED DOME SCJ-200;
- видео камера сетевая SPEED DOME Beward BD75-5;

- уличная видеокамера SPEED.
- Стенд "Системы видеонаблюдения" в составе:
- видеорегистратор DHI-NVR4216-16P-4KS2;
- источник бесперебойного питания UPS 400VA Ippon Back.
- Стенд "Пожарно-охранные сигнализации" в составе:
- охранное устройство Мираж-GSMA4-03;
- ИК извещатель "РАПИД";
- ИК извещатель "ФОТОН";
- Извещатель радиоволновый Астра-552;
- Комбинированный извещатель Астра-8;
- Извещатель ИПД-3.1М;
- Климатическая станция Vantage PRO2.
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.4. Материально-техническое и программное обеспечение для курсовой работы

Аудитория моделирования, проектирования и эксплуатации информационных и аналитических систем: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 407 ауд.

Описание имеющегося оборудования:

- Интерактивная доска TraceBoard TS-408L;
- Проектор ViewSonic PJD5154 DLP;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.5. 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.

8.6. 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 Теоретические вопросы защиты информации и	ОПК-1, ОПК-2	Отчет по курсовой работе	Примерный перечень тематик курсовых работ
построения информационных систем		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
2 Проектирование автоматизированных	ОПК-1, ОПК-2	Отчет по курсовой работе	Примерный перечень тематик курсовых работ
информационных систем		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
3 Содержание работ на этапах создания автоматизированных	ОПК-1, ОПК-2	Отчет по курсовой работе	Примерный перечень тематик курсовых работ
информационных систем		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий

4 Способы и методы защиты информации в	ОПК-1, ОПК-2	Отчет по курсовой работе	Примерный перечень тематик курсовых работ
информационных системах		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
5 Средства разработки и тестирования автоматизированных	ОПК-1, ОПК-2	Отчет по курсовой работе Лабораторная	Примерный перечень тематик курсовых работ Темы лабораторных работ
информационных систем		работа	Tembrandopuroprism pucor
		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

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

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3. Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

0	*
Оценка	Формулировка требований к степени компетенции

2	Не имеет необходимых представлений о проверяемом материале
(неудовлетворительно)	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	Знать и уметь на репродуктивном уровне. Обучающихся знает
(удовлетворительно)	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. К правовым методам, обеспечивающим информационную безопасность, относятся:
 - 1. Разработка аппаратных средств обеспечения правовых данных
 - 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
 - 3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности
- 2. Основными источниками угроз информационной безопасности являются все указанное в списке:
 - 1. Хищение жестких дисков, подключение к сети, инсайдерство
 - 2. Перехват данных, хищение данных, изменение архитектуры системы
 - 3. Хищение данных, подкуп системных администраторов, нарушение регламента работы
- 3. Угроза информационной системе (компьютерной сети) это:
 - 1. Вероятное событие
 - 2. Детерминированное (всегда определенное) событие
 - 3. Событие, происходящее периодически
- 4. Для чего предназначены информационные системы автоматизированного проектирования?
 - 1. для автоматизации функций управленческого персонала.
 - 2. для автоматизации любых функций компании и охватывают весь цикл работ от проектирования до сбыта продукции
 - 3. для автоматизации функций производственного персонала.
 - 4. для автоматизации работы при создании новой техники или технологии.
- 5. Информационная система (ИС) это:
 - 1. это совокупность условий, средств и методов на базе компьютерных систем, предназначенных для создания и использования информационных ресурсов.
 - 2. это совокупность программных продуктов, установленных на компьютере, технология работы в которых позволяет достичь поставленную пользователем цель.
 - 3. это взаимосвязанная совокупность средств, методов и персонала, используемых для об-

работки данных.

- 4. это совокупность данных, сформированная производителем для ее распространения в материальной или в нематериальной форме.
- 5. это процесс, определяемый совокупностью средств и методов обработки, изготовления, изменения состояния, свойств, формы сырья или материала.
- 6. это процесс, использующий совокупность средств и методов обработки и передачи данных и первичной информации для получения информации нового качества о состоянии объекта.

процесса или явления.

- 6. Методика тестирования на проникновение называется:
 - 1. Аудит
 - 2. Пентест
 - 3. Honeypot
 - 4. Metasploit
- 7. Что из перечисленного не является целью проведения аудита безопасности?
 - 1. Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов системы
 - 2. Выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности системы
 - 3. Оценка будущего уровня защищенности системы
 - 4. Оценка соответствия системы существующим стандартам в области информационной безопасности.
- 8. К какой категории охраняемой информации относится врачебная тайна?
 - 1. государственная тайна
 - 2. служебная тайна
 - 3. профессиональная тайна
 - 4. объекты авторского права
- 9. Какой институт в США занимается вопросами информационной безопасности, разрабатывая стандарты и технологии в этой области?
 - 1. PIST
 - 2. NIST
 - 3. DAST
 - 4. ANB
- 10. Как называется разновидность DDOS атаки при которой атакующий шлёт маленький по объё-му HTTP-пакет, но такой, чтобы сервер ответил на него пакетом, размер которого в сотни раз больше?
 - 1. НТТР-флуд
 - 2. Ping-флуд
 - 3. Smurf-атака
 - 4. Aтака Fraggle
 - 5. SYN-флуд
- 11. Как называется разновидность DDOS атаки при которой атакующий шлёт ICMPсообщения через усиливающую сеть?
 - 1. НТТР-флуд
 - 2. Ping-флуд
 - 3. Smurf-атака
 - 4. Aтака Fraggle
 - 5. SYN-флуд
- 12. Как называется разновидность DDOS атаки при которой атакующий шлёт UDP пакеты через усиливающую сеть?

- 1. НТТР-флуд
- 2. Ping-флуд
- 3. Smurf-атака
- 4. Aтака Fraggle
- 5. SYN-флуд
- 13. Как называется разновидность DDOS атаки при которой атакующий подменяет свой IP адрес на несуществующий при установки соединения?
 - 1. НТТР-флуд
 - 2. Ping-флуд
 - 3. Smurf-атака
 - 4. Aтака Fraggle
 - 5. SYN-флуд
- 14. Как называется атака. которая осуществляется путём размещения на веб-странице ссылки или скрипта, пытающегося получить доступ к сайту, на котором атакуемый пользователь заве-домо (или предположительно) уже аутентифицирован.
 - 1. DDOS
 - 2. CSRF
 - 3. XSS
 - 4. CORS
- 15. Как называется механизм безопасности, который позволяет веб-странице из одного домена об-ращаться к ресурсу с другим доменом (кросс-доменным запросом)?
 - 1. XSS
 - 2. JSONP
 - 3. OWASP
 - 4. CORS

9.1.2. Перечень экзаменационных вопросов

- 1. Общие определения и характеристики систем. Понятие сложности, критерии и свойства.
- 2. Критерии и свойства для системы. Вероятностная модель системы и пример пограничных состояний.
- 3. Информационные системы. Автоматизированные системы. Определения. Структура и классификация систем.
- 4. Базовые информационные процессы в системах.
- 5. Закон необходимого разнообразия Эшби. Энтропийная форма закона. Следствия из закона Эшби.
- 6. Основные принципы обеспечения информационной безопасности для информационных систем.
- 7. Методическая и нормативная база для построения защищенных систем.
- 8. Виды защищенных автоматизированных систем в соответствии с требованиями ГОСТ.
- 9. Принципы защиты информации в автоматизированных системах в соответствии с требованиями ГОСТ.
- 10. Принципы защиты информации в ИСПДН.
- 11. Аспекты построения доверенной вычислительной среды (ТСВ).
- 12. Способы реализации механизмов парольной защиты. Хранение и передача паролей.
- 13. Принципы распределения и реализации системы полномочий и доступов.
- 14. Пример построения защищенной системы на основе микроядерной ОС.
- 15. Программные аспекты построения защищенных систем. Работа с памятью.
- 16. Общие принципы обеспечения резервирования и защиты от сбоев.
- 17. Протоколы резервирования сетевой инфраструктуры.
- 18. Аспекты резервирования и надежности виртуальных систем.
- 19. Иерархическая модель данных.
- 20. Сетевая модель данных.
- 21. Реляционная модель данных.

- 22. Модель данных «Сущность-Связь».
- 23. Модель системы защиты. Комплексный подход.
- 24. Международные стандарты оценки защищённости.
- 25. Руководящие документы Гостехкомиссии России

9.1.3. Примерный перечень вопросов для защиты курсовой работы

- 1. Технология IDEF0 и ее применение для построения модели "черный ящик".
- 2. Реестры сертифицированных средств защиты информации.
- 3. Критерии оценки безопасности информационных технологий.
- 4. Оценочные уровни доверия.
- 5. Анализ СЗИ с использованием ГОСТ Р ИСО/МЭК 15408-3.

9.1.4. Примерный перечень тематик курсовых работ

- 1. web-ориентированная информационная система;
- 2. информационная система персональных данных;
- 3. персональная информационная система;
- 4. корпоративная информационная система;
- 5. медицинская информационная система.

9.1.5. Темы практических занятий

- 1. Разработка технического задания на защищенную информационную систему
- 2. Анализ сертифицированного СЗИ на предмет его функциональных возможностей. Построение модели типа «черный ящик» для исследуемой системы с последующей детализацией по технологии IDEF0.
- 3. Анализ СЗИ с использованием ГОСТ Р ИСО/МЭК 15408-3-2008«Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения» на предмет оценочных уровней доверия.
- 4. Обеспечение информационной безопасности в информационных системах

9.1.6. Темы лабораторных работ

1. Проектирование автоматизированной системы с учетом государственных стандартов. Анализ реализации модулей автоматизированных систем.

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	Преимущественно письменная	
	самостоятельные работы, вопросы	проверка	
	к зачету, контрольные работы		
С нарушениями зрения	Собеседование по вопросам к	Преимущественно устная	
	зачету, опрос по терминам	проверка (индивидуально)	
С нарушениями опорно-	Решение дистанционных тестов,	Преимущественно	
двигательного аппарата	контрольные работы, письменные	дистанционными методами	
	самостоятельные работы, вопросы		
	к зачету		
С ограничениями по	Тесты, письменные	Преимущественно проверка	
общемедицинским	самостоятельные работы, вопросы	методами, определяющимися	
показаниям	к зачету, контрольные работы,	исходя из состояния	
	устные ответы	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.

24

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 КИБЭВС протокол № 1 от «25 » 1 2022 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa- 9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa- 9347-a5e4dbb90e8d
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	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234- 88f9-e1597aac6463
РАЗРАБОТАНО:		
Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863- b293-f03438cb07cc