МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА»

УТВЕРЖДАЮ
и.о. декана _____ Батчаева М.Д.
«___» _____ 2024 г.
М.П.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ
ПО
ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ
ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

«СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ»

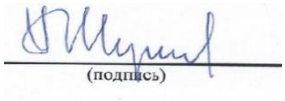
Карачаевск- 2024

Составитель: ст. преп. каф. ИВМ Аргуянова Альбина Борисовна

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по дополнительной профессиональной образовательной программе профессиональной переподготовки «Системное администрирование информационно-коммуникационных систем», профстандартом (Приказ Минтруда России от 29.09.2020 N 680н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем" (Зарегистрировано в Минюсте России 26.10.2020 N 60580))., локальными актами КЧГУ.

Рабочая программа рассмотрена и утверждена на заседании кафедры информатики и вычислительной математики на 2023-2024 уч. год.

Протокол № 1 от 29.01. 2024 г.

Заведующий кафедрой  к. ф.-м. н., доц. Шунгаров Х.Д.

Содержание

1. Наименование дисциплины (модуля)

Безопасность информационных технологий и систем

Целью освоения дисциплины является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Для достижения цели ставятся задачи:

- формирование умения обеспечить защиту информации и объектов информатизации;
- формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов;
- формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия; настройка и обслуживание аппаратно-программных средств.

В результате освоения дисциплины обучающийся должен:

Знать: современные информационно-коммуникационные технологии и возможности их обезопасить;

Уметь: пользоваться методикой применения информационно-коммуникационных технологий в решении задач профессиональной деятельности.

Владеть: навыками освоения и применения информационно-коммуникационных технологии с учетом требований информационной безопасности.

Цели и задачи дисциплины определены в соответствии с требованиями Федерального государственного образовательного в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденным приказом Министерства образования и науки Российской Федерации от 13.08.2020 г. №1016, дополнительной профессиональной образовательной программе профессиональной переподготовки «Системное администрирование информационно-коммуникационных систем».

2. Место дисциплины в структуре дополнительной профессиональной образовательной программы профессиональной переподготовки «*Безопасность информационных технологий и систем*»

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ «*Безопасность информационных технологий и систем*». Индекс 05.
Требования к предварительной подготовке обучающегося:
Для успешного освоения дисциплины студент должен иметь базовые знания по архитектуре информационных систем, принципам стандартизации в области управления проектами, состав международных инациональных стандартов управления проектами;
Требования к результатам освоения.
Дисциплина участвует в формировании компетенций ПК-1, ПК-3

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения ДПОП ПП обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

Код и содержание компетенции в соответствии с ФГОС ВО/ ПООП/	Индикаторы достижения компетенций	Декомпозиция индикаторов (результаты обучения - знания, умения, навыки)

ООП		
ПК-1: Способность выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.	ПК-1.1. Знать: методологии разработки программного обеспечения, назначение и возможности средств проектирования программного обеспечения.	**ПК-1.1.1. Знает** как анализировать задачу и её базовые составляющие в соответствии с заданными требованиями **ПК-1.1.2. Умеет** как осуществлять поиск информации, интерпретировать и ранжировать её для решения поставленной задачи по различным типам запросов **ПК-1.1.3. Владеет** при обработке информации отличать факты от мнений, интерпретаций, оценок, формировать собственные мнения и суждения, аргументирует свои выводы и точку зрения
	ПК-1.2. Уметь: разрабатывать функциональные и иные требования к программным и программно-аппаратным средствам, осуществлять документирование на всех этапах проектирования и разработки, анализировать или самостоятельно разрабатывать требования к программному обеспечению; проектировать программные продукты для решения практических задач согласно разработанным требованиям; создавать программное обеспечения согласно разработанным проектам.	**ПК-1.2.1. Знает** как выбирать методы и средства решения задачи и анализирует методологические проблемы, возникающие при решении задачи **ПК-1.2.2. Умеет** рассматривать и предлагать возможные варианты решения поставленной задачи, оценивая их достоинства и недостатки; **ПК-1.2.3. Владеет** навыками разрабатывать и применять технологии языки программирования и работы с базами данных
	ПК-1.3. Иметь навыки: разработки требований к программным продуктам; использования методов и средств проектирования программного обеспечения;	**ПК-1.3.1. Знает** как отладить и протестировать программу с помощью языков программирования. **ПК-1.3.2. Умеет** составлять программы в высокоуровневых средах программирования; **ПК-1.3.3 Владеет** навыками программирования и ведения баз данных и информационных хранилищ

	создания программного обеспечения по разработанным проектам для решения практических и профессиональных задач. Проектирует программные интерфейсы, структуры и базы данных	
ПК-2: Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе	**ПК-2.1** Анализирует исходную информацию о запросах и потребностях заказчика применительно к информационной системе, документирует собранные данные в соответствии с регламентами организации информации	**ПК-2.1.1 Знает** основы управления взаимоотношения с клиентами и заказчиками; **ПК-2.1.2 Умеет** применять методы и средства управления ИТ проектами; **ПК-2.1.3. Владеет** основами управления структур и анализа базами данных;
	ПК-2.2. Документирует существующие бизнес-процессы организации заказчика, разрабатывает модели бизнес-процессов заказчика и адаптирует бизнес-процессы заказчика к возможностям информационной системы	**ПК-2.2.1. Знает как** анализировать исходную информацию о запросах и потребностях заказчика применительно к программным продуктам; **ПК-2.2.2. Умеет** документировать собранные данные в соответствии с регламентами организации информации; **ПК-2.2.3. Владеет** навыками работы в программах в которых можно собирать данные, анализировать потребности заказчика
	ПК-2.3. Демонстрирует знания по основам управления взаимоотношения с клиентами и заказчиками	**ПК-2.3.1 Знает** как осуществляется документооборот существующих бизнес-процессов организации заказчика; **ПК-2.3.2. Умеет** работать в соответствующих поставленным задачам программах; **ПК-2.3.3. Владеет** навыками самостоятельной научно-исследовательской деятельности в области проведения поиска и отбора информации, моделирования информационных систем;

	ПК-2.4. Применяет методы выявления требований, методы и средства управления ИТ проектами.	**ПК-2.4.1 Знает** с помощью каких методов выявления требований осуществляется работа с заказчиком; **ПК-2.4.2. Умеет** работать в программах, которые отвечают требованиям и поставленным задачам заказчика; **ПК-2.4.3. Владеет** навыками работы со средствами управления ИТ проектами

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины (модуля) составляет 72 академических часа.

Объём дисциплины	***Всего часов***
Общая трудоемкость дисциплины	**72**
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)	28
Аудиторная работа (всего):	**28**
лекции	14
семинары, практические занятия	14
практикумы	-
лабораторные работы	-
Внеаудиторная работа:	
курсовые работы	
консультация перед экзаменом	
Самостоятельная работа обучающихся (всего)	**44**
Контроль	
Вид промежуточной аттестации обучающегося (зачет / экзамен)	**Зачет**

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Раздел дисциплины	Общ. Труд. (в часах)	**Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)**				
		Всего	Ауд. уч. занятия		С\Р	План. результ. Обуч-я	Формы текущего контроля
			Лек.	Пр./ сем			
1	**Раздел 1. Основные понятия и положения защиты информации в компьютерных системах**	**12**	**2**	**2**	**8**		
1.1	Понятия экономической и информационной безопасности. Ключевые вопросы ИБ. Экономическая и информационная безопасность. Составляющие информационной безопасности.		**2**			ПК-1, ПК-3	Задания по теме лекции
1.2	Основы законодательства в области обеспечения информационной безопасности			2		ПК-1, ПК-3	Задания по теме занятия.
1.3	Краткий обзор зарубежного законодательства в области информационной безопасности. Российское законодательство в области информационной безопасности. Закон «Об информации, информационных технологиях и защите информации». Другие законы и нормативные акты.				8	ПК-1, ПК-3	Реферат
2	**Раздел 2. Направления обеспечения информационной безопасности.**	**12**	**2**	**2**	**8**		
2.1	Программные средства защиты. Криптографические средства защиты.		2			ПК-1, ПК-3	Задания по теме лекции
2.2	Хакерские утилиты и прочие вредоносные программы. Классические компьютерные вирусы. Скрипт-вирусы. Троянские программы. Сетевые черви.			2		ПК-1, ПК-3	Задания по теме занятия.

2.3	Идентификация и аутентификация. Парольная зашита.				8	ПК-1, ПК-3	Реферат
3	**Раздел 3. Построения системы информационной безопасности**	**12**	**2**	**2**	**8**		
3.1	Основные аспекты построения системы информационной безопасности. Программа информационной безопасности. Модели ИБ, требования и основные этапы реализации информационной безопасности.		2			ПК-1, ПК-3	Задания по теме лекции
3.2	Мероприятия по защите информации. Политика информационной безопасности.			2		ПК-1, ПК-3	Задания по теме занятия.
3.3	Анализ и управление рисками при реализации информационной безопасности. Соотношение эффективности и рентабельности систем информационной безопасности.				8	ПК-1, ПК-3	Реферат
4	**Раздел 4. Защита информации в информационных системах и компьютерных сетях**	**12**	**2**	**2**	**8**		
4.1	Определение защищенной информационной системы. Требования к архитектуре ИС для обеспечения безопасности ее функционирования		**2**			ПК-1, ПК-3	Задания по теме лекции
4.2	Методология анализа защищенности информационной системы.			2		ПК-1, ПК-3	Задания по теме занятия.
4.3	Концепция защищенных виртуальных частных сетей.				8	ПК-1, ПК-3	Реферат
5	**Раздел 5. Защита информации от утечки по техническим каналам**	**8**	**2**	**2**	**4**		
5.1	Способы защиты информации. Характеристика защитных действий.		2			ПК-1, ПК-3	Задания по теме лекции
5.2	Защита информации от утечки по визуально-оптическим каналам. Защита информации от утечки по акустическим каналам. Защита информации от утечки по электромагнитным.			2		ПК-1, ПК-3	Задания по теме занятия.
5.3	Защита информации от утечки по материально-вещественным каналам.				4	ПК-1, ПК-3	Реферат

6	**Раздел 6. Противодействие несанкционированному доступу к источникам конфиденциальной информации**	8	2	2	4		
6.1	Способы несанкционированного доступа. Технические средства несанкционированного доступа к информации. Защита от наблюдения и фотографирования. Защита от подслушивания.		2			ПК-1, ПК-3	Задания по теме лекции
6.2	Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра.			2		ПК-1, ПК-3	Задания по теме занятия.
6.3	Передача зашифрованных сообщений по электронной почте.				4	ПК-1, ПК-3	Реферат
7	**Раздел 7. Защита информации в электронных платежных системах**	**8**	**2**	**2**	**4**		
7.1	Принципы функционирования электронных платежных систем. Электронные пластиковые карты.		**2**			ПК-1, ПК-3	Задания по теме лекции
7.2	Персональный идентификационный номер. Универсальная электронная платежная система UEPS.			**2**		ПК-1, ПК-3	Задания по теме занятия.
7.3	Обеспечение безопасности электронных платежей через сеть Internet.				**4**	ПК-1, ПК-3	Реферат
Всего по видам учебных занятий		**48**	**14**	**14**	**44**		

5.2. Виды занятий и их содержание

5.2.1. Тематика и краткое содержание лекционных занятий

Лекция № 1

Тема: **Понятия экономической и информационной безопасности**.

Основные вопросы, рассматриваемые на занятии**:**

1. Основные понятия и определения.
2. Ключевые вопросы ИБ.
3. Экономическая и информационная безопасность.
4. Составляющие информационной безопасности..

Лекция № 2

Тема: Программные средства защиты. Криптографические средства защиты

Основные вопросы, рассматриваемые на занятии:

1. Программные средства защиты.
2. Криптографические средства защиты.
3. Хакерские утилиты и прочие вредоносные программы.

Лекция №3

Тема: Построения системы информационной безопасности

Основные вопросы, рассматриваемые на занятии:

1. Основные аспекты построения системы информационной безопасности.
2. Программа информационной безопасности.

3. Модели ИБ, требования и основные этапы реализации информационной безопасности.

Лекция №4

Тема: Защита информации в информационных системах и компьютерных сетях

Основные вопросы, рассматриваемые на занятии:

1. Определение защищенной информационной системы.
2. Требования к архитектуре ИС для обеспечения безопасности ее функционирования.

Лекция №5

Тема: Защита информации от утечки по техническим каналам

Основные вопросы, рассматриваемые на занятии:

1. Способы защиты информации.
2. Характеристика защитных действий.
3. Защита информации от утечки по визуально-оптическим каналам.

Лекция № 6

Тема: Противодействие несанкционированному доступу к источникам конфиденциальной информации.

Основные вопросы, рассматриваемые на занятии:

1. Способы несанкционированного доступа.
2. Технические средства несанкционированного доступа к информации.
3. Защита от наблюдения и фотографирования.
4. Защита от подслушивания.

Лекция №7

Тема: Защита информации в электронных платежных системах

Основные вопросы, рассматриваемые на занятии:

1. Принципы функционирования электронных платежных систем.
2. Электронные пластиковые карты.
3. Персональный идентификационный номер.

5.2.2 Тематика и содержание семинарских занятий по курсу:

Практическое занятие № 1

Тема: Основные понятия и положения защиты информации в компьютерных системах

Основные вопросы, рассматриваемые на занятии**:**

1. Основы законодательства в области обеспечения информационной безопасности.
2. Краткий обзор зарубежного законодательства в области информационной безопасности.

Практическое занятие № 2

Тема: Направления обеспечения информационной безопасности

Основные вопросы, рассматриваемые на занятии:

1. Программные средства защиты. Криптографические средства защиты.
2. Хакерские утилиты и прочие вредоносные программы.
3. Классические компьютерные вирусы. Скрипт-вирусы. Троянские программы. Сетевые черви..

Практическое занятие № 3

Тема: Построения системы информационной безопасности

Основные вопросы, рассматриваемые на занятии:

1. Мероприятия по защите информации.
2. Политика информационной безопасности.
3. Модели ИБ, требования и основные этапы реализации информационной безопасности.

Практическое занятие № 4

Тема: Защита информации в информационных системах и компьютерных сетях

Основные вопросы, рассматриваемые на занятии:

1. Методология анализа защищенности информационной системы.
2. Требования к архитектуре ИС для обеспечения безопасности ее функционирования.

Практическое занятие № 5

Тема: Защита информации от утечки по техническим каналам

Основные вопросы, рассматриваемые на занятии:

1. Защита информации от утечки по визуально-оптическим каналам.
2. Защита информации от утечки по акустическим каналам.
3. Защита информации от утечки по электромагнитным..

Практическое занятие № 6

Тема: Противодействие несанкционированному доступу к источникам конфиденциальной информации

Основные вопросы, рассматриваемые на занятии:

1. Технические средства несанкционированного доступа к информации.
2. Защита от копирования.
3. Привязка к аппаратному обеспечению.
4. Использование реестра.

Практическое занятие № 7

Тема: Защита информации в электронных платежных системах

Основные вопросы, рассматриваемые на занятии:

1. Персональный идентификационный номер.
2. Универсальная электронная платежная система UEPS;
3. Обеспечение безопасности электронных платежей через сеть Internet.

5.2. Тематика лабораторных занятий

Учебным планом не предусмотрены

5.3. Примерная тематика курсовых работ

Учебным планом не предусмотрены

5.4. Самостоятельная работа и контроль успеваемости

В рамках указанного в учебном плане объема самостоятельной работы по данной дисциплине (в часах) предусматривается выполнение следующих видов учебной деятельности:

Вид самостоятельной работы	Примерная трудоемкость
Проработка учебного материала занятий лекционного и семинарского типа	28
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	-
Самостоятельное изучение отдельных вопросов тем дисциплины, не рассматриваемых на занятиях лекционного и семинарского типа	44
Подготовка к текущему контролю	-
Поиск, изучение и презентация информации по заданной теме, анализ научных источников по заданной проблеме	-
Решение задач	-
Подготовка к промежуточной аттестации	-
Итого СРО	72 часов

6. Образовательные технологии

При проведении учебных занятий по дисциплине используются традиционные и инновационные, в том числе информационные образовательные технологии, включая при необходимости применение активных и интерактивных методов обучения.

Традиционные образовательные технологии реализуются, преимущественно, в процессе лекционных и практических (семинарских, лабораторных) занятий. Инновационные образовательные технологии используются в процессе аудиторных занятий и самостоятельной работы студентов в виде применения активных и интерактивных методов обучения.

Информационные образовательные технологии реализуются в процессе использования электронно-библиотечных систем, электронных образовательных ресурсов и элементов электронного обучения в электронной информационно-образовательной среде для активизации учебного процесса и самостоятельной работы студентов.

Развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений и лидерских качеств при проведении учебных занятий.

Практические (семинарские занятия относятся к интерактивным методам обучения и обладают значительными преимуществами по сравнению с традиционными методами обучения, главным недостатком которых является известная изначальная пассивность субъекта и объекта обучения.

Практические занятия могут проводиться в форме групповой дискуссии, «мозговой атаки», разборка кейсов, решения практических задач и др. Прежде, чем дать группе информацию, важно подготовить участников, активизировать их ментальные процессы, включить их внимание, развивать кооперацию и сотрудничество при принятии решений.

Методические рекомендации по проведению различных видов практических (семинарских) занятий.

1.Обсуждение в группах

Групповое обсуждение какого-либо вопроса направлено на нахождении истины или достижение лучшего взаимопонимания, Групповые обсуждения способствуют лучшему усвоению изучаемого материала.

На первом этапе группового обсуждения перед обучающимися ставится проблема, выделяется определенное время, в течение которого обучающиеся должны подготовить аргументированный развернутый ответ.

Преподаватель может устанавливать определенные правила проведения группового обсуждения:

-задавать определенные рамки обсуждения (например, указать не менее 5…. 10 ошибок);

-ввести алгоритм выработки общего мнения (решения);

-назначить модератора (ведущего), руководящего ходом группового обсуждения.

На втором этапе группового обсуждения вырабатывается групповое решение совместно с преподавателем (арбитром).

Разновидностью группового обсуждения является круглый стол, который проводится с целью поделиться проблемами, собственным видением вопроса, познакомиться с опытом, достижениями.

2.Публичная презентация проекта

Презентация – самый эффективный способ донесения важной информации как в разговоре «один на один», так и при публичных выступлениях. Слайд-презентации с использованием мультимедийного оборудования позволяют эффективно и наглядно представить содержание изучаемого материала, выделить и проиллюстрировать сообщение, которое несет поучительную информацию, показать ее ключевые содержательные пункты. Использование интерактивных элементов позволяет усилить эффективность публичных выступлений.

3.Дискуссия

Как интерактивный метод обучения означает исследование или разбор. Образовательной дискуссией называется целенаправленное, коллективное обсуждение конкретной проблемы (ситуации), сопровождающейся обменом идеями, опытом, суждениями, мнениями в составе группы обучающихся.

Как правило, дискуссия обычно проходит три стадии: ориентация, оценка и консолидация. Последовательное рассмотрение каждой стадии позволяет выделить следующие их особенности.

Стадия ориентации предполагает адаптацию участников дискуссии к самой проблеме, друг другу, что позволяет сформулировать проблему, цели дискуссии; установить правила, регламент дискуссии.

В стадии оценки происходит выступление участников дискуссии, их ответы на возникающие вопросы, сбор максимального объема идей (знаний), предложений, пресечение преподавателем (арбитром) личных амбиций отклонений от темы дискуссии.

Стадия консолидации заключается в анализе результатов дискуссии, согласовании мнений и позиций, совместном формулировании решений и их принятии.

В зависимости от целей и задач занятия, возможно, использовать следующие виды дискуссий: классические дебаты, экспресс-дискуссия, текстовая дискуссия, проблемная дискуссия, ролевая (ситуационная) дискуссия.

7. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

7.1 Описание шкал оценивания степени сформированности компетенций

Уровни сформированности компетенций	Индикаторы	Качественные критерии оценивание			
		2 балла	3 балла	4 балла	5 баллов
ПК-3					
Базовый	ПК-3.1 Знать: методы и средства защиты от несанкционированного доступа в ИКС; современные средства контроля и диагностики параметров ИКС; требования к информационной безопасности; методологию взаимодействия открытых систем и сетевые протоколы ПК-3.2 Умеет: анализировать текущие процессы,	Не знает	В целом знает	Знает	

	выделять основные операции и определять участки, требующие автоматизации и оптимизации с применением больших данных; проводить моделирование процессов и систем с применением современных инструментальных средств; обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы ПК-3.3 Владеть: навыками конфигурации механизма разграничения прав доступа операционной системы; навыками самостоятельной научно-исследовательской деятельности в области проведения поиска и от бора информации, моделирования информационных систем; навыками стандартизации процессов в области больших данных при проектировании ИС.				
	ПК-3.1 Знать: методы и средства защиты от несанкционированного доступа в ИКС; современные средства контроля и диагностики параметров ИКС; требования к информационной безопасности; методологию взаимодействия открытых систем и сетевые протоколы ПК-3.2 Умеет: анализировать текущие процессы, выделять основные операции и определять участки, требующие автоматизации и оптимизации с применением больших данных; проводить моделирование процессов и систем с применением современных инструментальных средств; обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы ПК-3.3 Владеть: навыками конфигурации механизма разграничения прав доступа операционной системы; навыками самостоятельной научно-исследовательской деятельности в области проведения поиска и от бора информации, моделирования информационных систем; навыками стандартизации процессов в области больших данных при проектировании ИС.	Не умеет	В целом умеет	Умеет	
	ПК-3.1 Знать: методы и средства защиты от несанкционированного доступа в ИКС; современные средства контроля и диагностики параметров ИКС; требования к информационной безопасности; методологию взаимодействия открытых систем и сетевые протоколы ПК-3.2 Умеет: анализировать текущие процессы, выделять основные операции и определять участки, требующие автоматизации и оптимизации с применением больших данных; проводить моделирование процессов и систем с применением современных инструментальных средств; обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы ПК-3.3 Владеть: навыками конфигурации механизма	Не владеет.	В целом владеет	Владеет	

	разграничения прав доступа операционной системы; навыками самостоятельной научно-исследовательской деятельности в области проведения поиска и от бора информации, моделирования информационных систем; навыками стандартизации процессов в области больших данных при проектировании ИС.				
Повышенный	ПК-3.1 Знать: методы и средства защиты от несанкционированного доступа в ИКС; современные средства контроля и диагностики параметров ИКС; требования к информационной безопасности; методологию взаимодействия открытых систем и сетевые протоколы ПК-3.2 Умеет: анализировать текущие процессы, выделять основные операции и определять участки, требующие автоматизации и оптимизации с применением больших данных; проводить моделирование процессов и систем с применением современных инструментальных средств; обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы ПК-3.3 Владеть: навыками конфигурации механизма разграничения прав доступа операционной системы; навыками самостоятельной научно-исследовательской деятельности в области проведения поиска и от бора информации, моделирования информационных систем; навыками стандартизации процессов в области больших данных при проектировании ИС.				В полном объеме знает
	ПК-3.1 Знать: методы и средства защиты от несанкционированного доступа в ИКС; современные средства контроля и диагностики параметров ИКС; требования к информационной безопасности; методологию взаимодействия открытых систем и сетевые протоколы ПК-3.2 Умеет: анализировать текущие процессы, выделять основные операции и определять участки, требующие автоматизации и оптимизации с применением больших данных; проводить моделирование процессов и систем с применением современных инструментальных средств; обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы ПК-3.3 Владеть: навыками конфигурации механизма разграничения прав доступа операционной системы; навыками самостоятельной научно-исследовательской деятельности в области проведения поиска и от бора информации, моделирования информационных систем; навыками стандартизации процессов в области больших данных при проектировании ИС.				В полном объеме умеет
	ПК-3.1 Знать: методы и средства защиты от несанкционированного доступа в ИКС; современные				В полном

	средства контроля и диагностики параметров ИКС; требования к информационной безопасности; методологию взаимодействия открытых систем и сетевые протоколы ПК-3.2 Умеет: анализировать текущие процессы, выделять основные операции и определять участки, требующие автоматизации и оптимизации с применением больших данных; проводить моделирование процессов и систем с применением современных инструментальных средств; обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы ПК-3.3 Владеть: навыками конфигурации механизма разграничения прав доступа операционной системы; навыками самостоятельной научно-исследовательской деятельности в области проведения поиска и от бора информации, моделирования информационных систем; навыками стандартизации процессов в области больших данных при проектировании ИС.				объеме владеет
	ПК-1				
Базовый	ПК-1.1. Знать: методологии разработки программного обеспечения, назначение и возможности средств проектирования программного обеспечения. ПК-1.2. Уметь: разрабатывать функциональные и иные требования к программным и программно-аппаратным средствам, осуществлять документирование на всех этапах проектирования и разработки, анализировать или самостоятельно разрабатывать требования к программному обеспечению; проектировать программные продукты для решения практических задач согласно разработанным требованиям; создавать программное обеспечения согласно разработанным проектам. Владеть: навыками разработки требований к программным продуктам; использования методов и средств проектирования программного обеспечения; создания программного обеспечения по разработанным проектам для решения практических и профессиональных задач. Проектирует программные интерфейсы, структуры и базы данных.	Не знает	В целом знает	Знает	
	ПК-1.1. Знать: методологии разработки программного обеспечения, назначение и возможности средств проектирования программного обеспечения. ПК-1.2. Уметь: разрабатывать функциональные и иные требования к программным и программно-аппаратным средствам, осуществлять документирование на всех этапах проектирования и разработки, анализировать или самостоятельно	Не умеет	В целом умеет	Умеет	

	разрабатывать требования к программному обеспечению; проектировать программные продукты для решения практических задач согласно разработанным требованиям; создавать программное обеспечения согласно разработанным проектам. ПК-1.3. Владеть: навыками разработки требований к программным продуктам; использования методов и средств проектирования программного обеспечения; создания программного обеспечения по разработанным проектам для решения практических и профессиональных задач. Проектирует программные интерфейсы, структуры и базы данных.				
	ПК-1.1. Знать: методологии разработки программного обеспечения, назначение и возможности средств проектирования программного обеспечения. ПК-1.2. Уметь: разрабатывать функциональные и иные требования к программным и программно-аппаратным средствам, осуществлять документирование на всех этапах проектирования и разработки, анализировать или самостоятельно разрабатывать требования к программному обеспечению; проектировать программные продукты для решения практических задач согласно разработанным требованиям; создавать программное обеспечения согласно разработанным проектам. ПК-1.3. Владеть: навыками разработки требований к программным продуктам; использования методов и средств проектирования программного обеспечения; создания программного обеспечения по разработанным проектам для решения практических и профессиональных задач. Проектирует программные интерфейсы, структуры и базы данных.	Не владеет.	В целом владеет	Владеет	
Повышенный	ПК-1.1. Знать: методологии разработки программного обеспечения, назначение и возможности средств проектирования программного обеспечения. ПК-1.2. Уметь: разрабатывать функциональные и иные требования к программным и программно-аппаратным средствам, осуществлять документирование на всех этапах проектирования и разработки, анализировать или самостоятельно разрабатывать требования к программному обеспечению; проектировать программные продукты для решения практических задач согласно разработанным требованиям; создавать программное обеспечения согласно разработанным проектам. ПК-1.3. Владеть: навыками разработки требований к программным продуктам; использования методов и средств проектирования программного обеспечения;				В полном объеме знает

	создания программного обеспечения по разработанным проектам для решения практических и профессиональных задач. Проектирует программные интерфейсы, структуры и базы данных.				
	ПК-1.1. Знать: методологии разработки программного обеспечения, назначение и возможности средств проектирования программного обеспечения. ПК-1.2. Уметь: разрабатывать функциональные и иные требования к программным и программно-аппаратным средствам, осуществлять документирование на всех этапах проектирования и разработки, анализировать или самостоятельно разрабатывать требования к программному обеспечению; проектировать программные продукты для решения практических задач согласно разработанным требованиям; создавать программное обеспечения согласно разработанным проектам. ПК-1.3. Владеть: навыками разработки требований к программным продуктам; использования методов и средств проектирования программного обеспечения; создания программного обеспечения по разработанным проектам для решения практических и профессиональных задач. Проектирует программные интерфейсы, структуры и базы данных.				В полном объеме умеет
	ПК-1.1. Знать: методологии разработки программного обеспечения, назначение и возможности средств проектирования программного обеспечения. ПК-1.2. Уметь: разрабатывать функциональные и иные требования к программным и программно-аппаратным средствам, осуществлять документирование на всех этапах проектирования и разработки, анализировать или самостоятельно разрабатывать требования к программному обеспечению; проектировать программные продукты для решения практических задач согласно разработанным требованиям; создавать программное обеспечения согласно разработанным проектам. ПК-1.3. Владеть: навыками разработки требований к программным продуктам; использования методов и средств проектирования программного обеспечения; создания программного обеспечения по разработанным проектам для решения практических и профессиональных задач. Проектирует программные интерфейсы, структуры и базы данных.				В полном объеме владеет

7.2. Типовые контрольные задания или иные учебно-методические материалы, необходимые для оценивания степени сформированности компетенций в процессе освоения учебной дисциплины

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними.
2. Современные средства защиты информации.
3. Современные системы компьютерной безопасности.
4. Современные средства противодействия экономическому шпионажу.
5. Современные криптографические системы.
6. Криптоанализ, современное состояние.
7. Правовые основы защиты информации.
8. Технические аспекты обеспечения защиты информации. Современное состояние.
9. Атаки на систему безопасности и современные методы защиты.
10. Современные пути решения проблемы информационной безопасности РФ.

Критерии оценки доклада, сообщения, реферата:

Отметка «отлично» за письменную работу, реферат, сообщение ставится, если изложенный в докладе материал:

- отличается глубиной и содержательностью, соответствует заявленной теме;
- четко структурирован, с выделением основных моментов;
- доклад сделан кратко, четко, с выделением основных данных;
- на вопросы по теме доклада получены полные исчерпывающие ответы.

Отметка «хорошо» ставится, если изложенный в докладе материал:

- характеризуется достаточным содержательным уровнем, но отличается недостаточной структурированностью;
- доклад длинный, не вполне четкий;
- на вопросы по теме доклада получены полные исчерпывающие ответы только после наводящих вопросов, или не на все вопросы.

Отметка «удовлетворительно» ставится, если изложенный в докладе материал:

- недостаточно раскрыт, носит фрагментарный характер, слабо структурирован;
- докладчик слабо ориентируется в излагаемом материале;
- на вопросы по теме доклада не были получены ответы или они не были правильными.

Отметка «неудовлетворительно» ставится, если:

- доклад не сделан;
- докладчик не ориентируется в излагаемом материале;
- на вопросы по выполненной работе не были получены ответы или они не были правильными.

7.2.1. Тестовые задания для промежуточной аттестации

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

ОПК-9
11) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность
- Доступность
- Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

Шкала оценивания *(за правильный ответ дается 1 балл)*

«неудовлетворительно» – 50% и менее
«удовлетворительно» – 51-80%
«хорошо» – 81-90%
«отлично» – 91-100%

7.2.2. Примерные вопросы к итоговой аттестации (зачет)

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Что включает борьба с атаками на уровне приложений?
11. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
12. В чем заключается распределенное хранение файлов?
13. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
14. Какие уровни информационной защиты существуют, их основные составляющие?
15. В чем заключаются задачи криптографии?
16. Зачем нужны ключи?
17. Какая схема шифрования называется многоалфавитной подстановкой?
18. Какие системы шифрования вы знаете?
19. Что включает в себя защита информации от несанкционированного доступа?
20. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
21. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
22. Какой процесс называется аутентификацией пользователя?
23. Какие схемы аутентификации вы знаете?
24. Какие требования предъявляются к современным криптографическим системам защиты информации?

ОПК-9

25. Какими способами можно проверить систему безопасности?

26.Что является основными характеристиками технических средств защиты информации?
27. Какие требования предъявляются к межсетевым экранам?
28. Какие имеются показатели защищенности межсетевых экранов?
29. Какие атаки системы снаружи вы знаете?
30. Какая программа называется вирусом?
31. Какая атака называется атакой отказа в обслуживании?
32. Какие виды вирусов вы знаете?
33. Как распространяются вирусы?
34. Какие методы обнаружения вирусов вы знаете?
35. Какие задачи решает система компьютерной безопасности?
36. Какие пути защиты информации в локальной сети существуют?
37. Какие задачи решают технические средства противодействия экономическому шпионажу?
38. Какие международные документы регламентируют деятельность по обеспечению защиты информации?
39.Что понимают под политикой информационной безопасности?
40. Что включает в себя политика информационной безопасности РФ?
41. Какие нормативные документы РФ определяют концепцию защиты информации?

Критерии оценки ответа на зачете по дисциплине

«Безопасность информационных технологий и систем»

✓ ***Зачтено*** - если ответ показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа.

✓ - знание узловых проблем программы и основного содержания лекционного курса; умение пользоваться концептуально-понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа.

✓ – фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.

✓ ***Не зачтено*** – незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

8.1. Основная литература:

1. Бабаш, А. В. История защиты информации в зарубежных странах: учебное пособие / А. В. Бабаш, Д. А. Ларин. - Москва: РИОР: ИНФРА-М,2020. - 284 с. - ISBN 978-5-369-01844-6. - URL: https://znanium.com /catalog/product/1081362

2. Башлы, П. Н. Информационная безопасность и защита информации : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222с. - ISBN 978-5-369-01178-2. - URL: https://znanium.com /catalog /product /405000
3. Баранова, Е. К. Основы информатики и защиты информации: учебное пособие / Е.К. Баранова Е.К. - М.: РИОР, ИНФРА-М, 2018. - 183 с. - ISBN 978-5-369-01169-0. - URL: https://znanium.com/catalog/ product /959916
4. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Москва: РИОР: ИНФРА-М, 2020. - 336 с. - ISBN 978-5-369-01761-6. - URL: https://znanium.com/catalog/product/1114032

8.2. Дополнительная литература:

1. Зашита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - ISBN 978-5-369-01759-3. - URL: https: //znanium.com/catalog /product/1018901
2. Информационная безопасность и защита информации: учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов; Государственный университет «Дубна». - Дубна: Государственный университет «Дубна», 2020. - 85 с. - ISBN 978-5-89847-608-3. URL: https: //e.lanbook. com /book /154490
3. Криптографическая защита информации: учебное пособие / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.] ; под редакцией С. О. Крамарова. - Москва: РИОР: ИНФРА-М, 2021. - 321 с. - ISBN 978-5-369-01716-6. - URL: https://znanium.com/catalog/product /1153156
4. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. — 3-е изд., испр. и доп. - Москва : ИНФРА-М, 2020. — 327 с. . - ISBN 978-5-16-015471-8. - URL: https: //znanium.com /catalog /product /1035570

9. Методические указания для обучающихся по освоению учебной дисциплины (модуля)

Вид учебных занятий	Организация деятельности студента
Лекция	Написание конспекта лекций: краткое, схематичное, последовательное фиксирование основных положений, выводов, формулировок, обобщений; выделение ключевых слов, терминов. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросы, терминов, материала, вызывающего трудности. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Конспектирование теоретических сведений. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, выполнение заданий.
Реферат	Реферат: Поиск литературы и составление библиографии, использование от 3 до 5 научных работ, изложение мнения авторов и своего суждения по выбранному вопросу; изложение основных аспектов проблемы. Ознакомиться со структурой и оформлением реферата.
Коллоквиум	Работа с конспектом лекций, подготовка ответов к контрольным вопросам и др.
Самостоятельная работа	Проработка учебного материала занятий лекционного и лабораторного типа. Изучение нового материала до его изложения на занятиях. Поиск, изучение

	и презентация информации по заданной теме, анализ научных источников. Самостоятельное изучение отдельных вопросов тем дисциплины, не рассматриваемых на занятиях лекционного и семинарского типа. Подготовка к текущему контролю, к промежуточной аттестации.
Подготовка к зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

10. Требования к условиям реализации рабочей программы дисциплины (модуля)

10.1. Общесистемные требования

Электронная информационно-образовательная среда ФГБОУ ВО «КЧГУ»
http://kchgu.ru - адрес официального сайта университета
https://do.kchgu.ru - электронная информационно-образовательная среда КЧГУ

Электронно-библиотечные системы (электронные библиотеки)

Учебный год	Наименование документа с указанием реквизитов	Срок действия документа
2023 / 2024 учебный год	Договор № 915 ЭБС ООО «Знаниум» от 12.05.2023г.	Действует до 15.05.2024 г.
	Электронно-библиотечная система «Лань». Договор № СЭБ НВ-294 от 1 декабря 2020 года.	Бессрочный
2023 / 2024 учебный год	Электронная библиотека КЧГУ (Э.Б.). Положение об ЭБ утверждено Ученым советом от 30.09.2015г. Протокол № 1). Электронный адрес: https: kchgu.ru/biblioteka - kchgu/	Бессрочный
2023 / 2024 учебный год	Электронно-библиотечные системы: Научная электронная библиотека «ELIBRARY.RU» - https://www.elibrary.ru. Лицензионное соглашение №15646 от 01.08.2014г. Бесплатно. Национальная электронная библиотека (НЭБ) – https://rusneb.ru. Договор №101/НЭБ/1391 от 22.03.2016г. Бесплатно. Электронный ресурс «Polred.com Обзор СМИ» – https://polpred.com. Соглашение. Бесплатно.	Бессрочно

10.2. Материально-техническое и учебно-методическое обеспечение дисциплины

При необходимости для проведения занятий используется аудитория, оборудованная компьютером с доступом к сети Интернет с установленным на нем необходимым программным обеспечением и браузером, проектор (интерактивная доска) для демонстрации презентаций и мультимедийного материала.

В соответствии с содержанием практических (лабораторных) занятий при их проведении используется аудитория, рабочие места обучающихся в которой оснащены компьютерной техникой, имеют широкополосный доступ в сеть Интернет и программное обеспечение, соответствующее решаемым задачам.

Рабочие места для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети Интернет и обеспечены доступом в электронную информационно-образовательную среду университета.

Занятия проходят в учебной аудитории № 27.

1. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Для проведения конференций

Специализированная мебель: столы ученические, стулья, стол преподавателя, доска меловая.

Технические средства обучения: персональный компьютер с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, звуковые колонки, проектор.

Лицензионное программное обеспечение:

Microsoft Windows (Лицензия № 60290784), бессрочная

Microsoft Office (Лицензия № 60127446), бессрочная

ABBY Fine Reader (лицензия № FCRP-1100-1002-3937), бессрочная

Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная

Google G Suite for Education (IC: 01i1p5u8), бессрочная

Антивирус Касперского. Действует до 03.03.2025г. (Договор № 56/2023 от 25 января 2023г.)

2. Читальный зал: для самостоятельной работы обучающихся; 80 мест, 10 компьютеров.

Специализированная мебель: столы ученические, стулья.

Технические средства обучения: Дисплей Брайля ALVA с программой экранного увеличителя MAGic Pro; стационарный видео увеличитель CIear View с монитором; 2 компьютерных роллера USB&PS/2; клавиатура с накладкой (ДЦП); акустическая система свободного звукового поля Front Row to Go/$; персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Лицензионное программное обеспечение:

Microsoft Windows (Лицензия № 60290784), бессрочная

Microsoft Office (Лицензия № 60127446), бессрочная

ABBY Fine Reader (лицензия № FCRP-1100-1002-3937), бессрочная

Calculate Linux (внесён в ЕРРП Пр иказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная

Google G Suite for Education (IC: 01i1p5u8), бессрочная

Антивирус Касперского. Действует до 03.03.2025г. (Договор № 56/2023 от 25 января 2023г.)

3. Научный зал: для самостоятельной работы, для научно-исследовательской работы обучающихся; 20 мест, 10 компьютеров

Специализированная мебель: столы ученические, стулья.

Технические средства обучения: персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Лицензионное программное обеспечение:

Microsoft Windows (Лицензия № 60290784), бессрочная

Microsoft Office (Лицензия № 60127446), бессрочная

ABBY Fine Reader (лицензия № FCRP-1100-1002-3937), бессрочная

Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная

Google G Suite for Education (IC: 01i1p5u8), бессрочная

Антивирус Касперского. Действует до 03.03.2025г. (Договор № 56/2023 от 25 января 2023г.)

10.3. Необходимый комплект лицензионного программного обеспечения

1. ABBY FineReader (лицензия №FCRP-1100-1002-3937), бессрочная.

2. Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная.

3. Google G Suite for Education (IC: 01i1p5u8), бессрочная.
4. Антивирус Касперского. Действует до 03.03.2025г. (Договор № 56/2023 от 25 января 2023г.)
5. Microsoft Office (лицензия №60127446), бессрочная.
6. Microsoft Windows (лицензия №60290784), бессрочная.

10.4. Современные профессиональные базы данных и информационные справочные системы

Современные профессиональные базы данных

1. Федеральный портал «Российское образование»- https://edu.ru/documents/
2. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) – http://school-collection.edu.ru/
3. Базы данных Scopus издательства Elsevir http://www.scopus.com/search/form.uri?display=basic.

Информационные справочные системы

1. Портал Федеральных государственных образовательных стандартов высшего образования - http://fgosvo.ru.
2. Федеральный центр информационно-образовательных ресурсов (ФЦИОР) – http://edu.ru.
3. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) – http://school-collection.edu.ru.
4. Информационная система «Единое окно доступа к образовательным ресурсам» (ИС «Единое окно») – http://window/edu.ru.
5. Информационная система «Информио».

11. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

В группах, в состав которых входят студенты с ОВЗ, в процессе проведения учебных занятий создается гибкая, вариативная организационно-методическая система обучения, адекватная образовательным потребностям данной категории обучающихся, которая позволяет не только обеспечить преемственность систем общего (инклюзивного) и высшего образования, но и будет способствовать формированию у них компетенций, предусмотренных ФГОС ВО, ускорит темпы профессионального становления, а также будет способствовать их социальной адаптации.

В процессе преподавания учебной дисциплины создается на каждом занятии толерантная социокультурная среда, необходимая для формирования у всех обучающихся гражданской, правовой и профессиональной позиции соучастия, готовности к полноценному общению, сотрудничеству, способности толерантно воспринимать социальные, личностные и культурные различия, в том числе и характерные для обучающихся с ОВЗ.

Посредством совместной, индивидуальной и групповой работы формируется у всех обучающихся активная жизненная позиции и развитие способности жить в мире разных людей и идей, а также обеспечивается соблюдение обучающимися их прав и свобод и признание права другого человека, в том числе и обучающихся с ОВЗ на такие же права.

В группах, в состав которых входят обучающиеся с ОВЗ, в процессе учебных занятий используются технологии, направленные на диагностику уровня и темпов профессионального становления обучающихся с ОВЗ, а также технологии мониторинга степени успешности формирования у них компетенций, предусмотренных ФГОС ВО при изучении данной учебной дисциплины, используя с этой целью специальные оценочные

материалы и формы проведения промежуточной и итоговой аттестации, специальные технические средства, предоставляя обучающимся с ОВЗ дополнительное время для подготовки ответов, привлекая тьютеров).

Материально-техническая база для реализации программы:

1. Мультимедийные средства:
- интерактивные доски «Smart Boarfd», «Toshiba»;
- экраны проекционные на штативе 280*120;
- мультимедиа-проекторы Epson, Benq, Mitsubishi, Aser.
2. Презентационное оборудование:
- радиосистемы AKG, Shure, Quik;
- видео комплекты Microsoft, Logitech;
- микрофоны беспроводные;
- класс компьютерный мультимедийный на 21 мест;
- ноутбуки Aser, Toshiba, Asus, HP.

Наличие компьютерной техники и специального программного обеспечения: имеются рабочие места, оборудованные рельефно-точечными клавиатурами (шрифт Брайля), программное обеспечение NVDA с функцией синтезатора речи, видео увеличителем, клавиатурой для лиц с ДЦП, роллером Распределение специализированного оборудования.

12.Лист регистрации изменений

В рабочей программе внесены следующие изменения:

Изменение	**Дата и номер протокола ученого совета факультета/ института, на котором были рассмотрены вопросы о необходимости внесения изменений**	**Дата и номер протокола ученого совета Университета, на котором были утверждены изменения**	**Дата введения изменений**
Обновлены договоры: 1). Антивирус Касперского. Действует до 03.03.2025г. (Договор № 56/2023 от 25 января 2023г.); 2). Договор №915 эбс ООО «Знаниум» от 12.05.2023г. Действует до 15.05.2024г.	27.06.2023г., протокол №10	Решение ученого совета КЧГУ от 29 июня 2023 года	29.06.2023 г.
Переутверждена ОП ВО. Обновлены РПД, РПП, РПВ, календарный план воспитания, программы ГИА, календарный график учебного процесса.	27.06.2023г., протокол №10	Решение ученого совета КЧГУ от 29 июня 2023 года	29.06.2023 г.