3++

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА»

Физико-математический факультет

Кафедра информатики и вычислительной математики

УТВЕРЖДАЮ
И. о. проректора по УР
М. Х. Чанкаев
«29» мая 2024 г., протокол № 8

Рабочая программа дисциплины

Защита информации

(наименование дисциплины (модуля)

Направление подготовки
09.03.01 Информатика и вычислительная техника
(шифр, название направления)

Направленность (профиль) подготовки
Системы автоматизированного проектирования

Квалификация выпускника
бакалавр

Форма обучения
Очная

Год начала подготовки
2022

Карачаевск, 2024

Составитель: старший преподаватель кафедры ИВМ Джаубаева З.К.

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.01. Информатика и вычислительная техника, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 №929 с изменениями и дополнениями от 26.11.2020г., №1456, 08.02.2021 г., №83, основной профессиональной образовательной программой высшего образования по направлению подготовки 09.03.01. Информатика и вычислительная техника, направленность(профиль); Системы автоматизированного проектирования, локальными актами КЧГУ.

Рабочая программа рассмотрена и утверждена на заседании кафедры

информатики и вычислительной математики на 2024-2025 уч. год, протокол № 9 от 07 мая 2024 г.

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

(подпись)

СОДЕРЖАНИЕ

1. Наименование дисциплины (модуля)

Защита информации

Целью изучения 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:

- получить представление о правилах защиты информации;
- изучить методы и средства обеспечения защиты информации
- изучить необходимый понятийный аппарат дисциплины;
- сформировать умение проводить анализ угроз безопасности;
- сформировать навыки защиты информации.

Цели и задачи дисциплины определены в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника (квалификация – бакалавр).

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Защита информации» (Б1.О.11) относится к обязательной части Б1.

Дисциплина (модуль) изучается на 4 курсе в 8 семестре.

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Индекс	Б1.О.11
Требования к предварительной подготовке обучающегося:	
Изучение данной дисциплины базируется на следующих курсах: «Информатика», «Дискретная математика», «Математическая логика и теория алгоритмов».	
Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Изучение дисциплины «Защита информации» необходимо для успешного прохождения итоговой государственной аттестации.	

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

Процесс изучения дисциплины «Защита информации» направлен на формирование следующих компетенций обучающегося:

Код компетенций	**Содержание компетенции в соответствии с ФГОС ВО/ ПООП/ ООП**	**Индикаторы достижения компетенций**	**Декомпозиция компетенций (результаты обучения) в соответствии с установленными индикаторами**
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной	**Знать:** Базовые понятия информатики и ИКТ, используемые в области защиты информации и обеспечения информационной безопасности; Современное состояние и тенденции развития методов и организационно-правовое обеспечение информационной

		безопасности. ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	безопасности; технологии эффективной защиты информации и информационной безопасности. **Уметь:** Классифицировать угрозы информационной безопасности объекта. **Владеть:** Основными методами защиты информации; практическими навыками организации защиты информации и обеспечения информационной безопасности.
ОПК-5	Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	ОПК-5.1. Знает основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем. ОПК-5.2. Умеет выполнять параметрическую настройку информационных и автоматизированных систем ОПК-5.3. Владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем	**Знать:** основные принципы аппаратно-программной защиты информации. **Уметь**: реагировать на различные угрозы информационной безопасности. **Владеть** навыками применения и настройки антивирусных систем и систем распознавания угроз и атак.

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 5 ЗЕТ, 180 академических часа.

Объём дисциплины	Всего часов	Всего часов
	для очной формы обучения	для заочной формы обучения
Общая трудоемкость дисциплины	180	
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)		

Аудиторная работа (всего):	72	
в том числе:		
лекции	24	
семинары, практические занятия	Не предусмотрено	
практикумы	Не предусмотрено	
лабораторные работы	48	
Внеаудиторная работа:		
консультация перед зачетом		
Внеаудиторная работа также включает индивидуальную работу обучающихся с преподавателем, групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем), творческую работу (эссе), рефераты, контрольные работы и др.		
Самостоятельная работа обучающихся (всего)	108	
Контроль самостоятельной работы		
Вид промежуточной аттестации обучающегося (зачет / экзамен)	экзамен	

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)

Для очной формы обучения

№ п/п	Раздел, тема дисциплины	Общая трудоемкость (в часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
		всего	Аудиторные уч. занятия			Сам. работа	Планируемые результаты обучения	Формы текущего контроля
			Лек	Пр	Лаб			
	Раздел 1. Общие положения информационной безопасности	**30**	**4**		**8**	**18**		
1.	Тема: Проблемы обеспечения информационной безопасности */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
2.	Тема: Составляющие информационной безопасности */ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
3.	Тема: Основы шифрования данных. */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
4.	Тема: История криптографии */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
5.	Тема: Угрозы информационной безопасности */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
6.	Тема: Методы реализации угроз информационной безопасности */ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
7.	Тема: Использование шифров замены для защиты	4			4		ОПК-3 ОПК-5	Отчет по лабораторной

	информации */лабз/*							работе
8.	Тема: Шифры однозначной замены. Полиграммные шифры */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
	Раздел 2. Нормативно-правовое обеспечение информационной безопасности	**30**	**4**		**8**	**18**		
9.	Тема: Нормативно-правовые основы информационной безопасности в РФ */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
10.	Тема: Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации */ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
11.	Тема: Шифры замены */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
12.	Тема: Омофонические шифры */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
13.	Тема: Основные виды «конфиденциальной» информации */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
14.	Тема: Информационная война */ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
15.	Тема: Шифры перестановки */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
16.	Тема: Шифры множественной перестановки */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
	Раздел 3. Криптографическая защита информации	**45**	**6**		**12**	**27**		
17.	Тема: Принципы криптографической защиты информации */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
18.	Тема: Основные требования к шифрам */ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
19.	Тема: Аддитивные шифры */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
20.	Тема: Аддитивное шифрование по модулю N */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
21.	Тема: Криптографические алгоритмы */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
22.	Тема: Шифры замены,	3				3	ОПК-3	Устный опрос

	перестановок, гаммирования, аналитические преобразования и композиционные */ср/*						ОПК-5	
23.	Тема: Комбинированные шифры */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
24.	Тема: Режимы адгоритма DES */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
25.	Тема: Электронная цифровая подпись */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
26.	Тема: Алгоритмы хэширования */ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
27.	Тема: Шифрование с открытым ключом. Алгоритм RSA */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
28.	Тема: Алгоритм RSA */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
	Раздел 4. Программно-аппаратная защита информации	**75**	**10**		**20**	**45**		
29.	Тема: Вредоносные программы и защита от них */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
30.	Тема: Факторы, определяющие качество антивирусных программ */ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
31.	Тема: Шифрование с открытым ключом. Алгоритм на основе задачи об укладке ранца */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
32.	Тема: Алгоритм на основе задачи об укладке ранца */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
33.	Тема: Механизмы обеспечения информационной безопасности в информационных системах */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
34.	Тема: Аутентификация на основе многоразовых и одноразовых паролей*/ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
35.	Тема: Шифрование с открытым ключом. Алгоритм шифрования Эль-Гамаля */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
36.	Тема: Алгоритм шифрования Эль-Гамаля */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
37.	Тема: Обеспечение информационной безопасности операционных систем */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос

38.	Тема: Основные функции подсистемы защиты операционной системы*/ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
39.	Тема: Оценка стойкости парольной защиты */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
40.	Тема: Количественная оценка стойкости парольной защиты */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
41.	Тема: Методы и средства защиты информации в сети Интернет */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
42.	Тема: Технологии межсетевых экранов */ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
43.	Тема: Управление криптоключами */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
44.	Тема: Алгоритм обмена ключами по схеме Диффи-Хеллмана */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
45.	Тема: Инженерно-техническая защита информации */лз/*	2	2				ОПК-3 ОПК-5	Устный опрос
46.	Тема: Организация режима секретности */ср/*	3				3	ОПК-3 ОПК-5	Устный опрос
47.	Тема: Программирование протоколов аутентификации пользователей */лабз/*	4			4		ОПК-3 ОПК-5	Отчет по лабораторной работе
48.	Тема: Одноразовые и многоразовые пароли */ср/*	6				6	ОПК-3 ОПК-5	Устный опрос
	Всего	**180**	**24**		**48**	**108**		

5.2. Тематика и краткое содержание лабораторных занятий

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 1-2

Тема: Основы шифрования данных.

Основные вопросы, рассматриваемые на занятии:

1) Проблемы защиты информации

2) Из истории криптографии

3) Методы шифрования

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 3-4

Тема: Использование шифров замены для защиты информации.

Основные вопросы, рассматриваемые на занятии:

1) Шифры однозначной замены

2) Полиграммные шифры

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 5-6

Тема: Шифры замены.

Основные вопросы, рассматриваемые на занятии:
1) Омофонические шифры
2) Полиалфавитные шифры

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 7-8

Тема: Шифры перестановки
Основные вопросы, рассматриваемые на занятии:
1) Шифры одинарной перестановки
2) Шифры множественной перестановки

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 9-10

Тема: Аддитивные шифры
Основные вопросы, рассматриваемые на занятии:
1) Гаммирование: длина периода гаммы, случайность распределения символов.
2) Аддитивное шифрование по модулю N.

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 11-12

Тема: Комбинированные шифры
Основные вопросы, рассматриваемые на занятии:
1) Методы блочного шифрования.
2) Шифр DES.

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 13-14

Тема: Шифрование с открытым ключом. Алгоритм RSA
Основные вопросы, рассматриваемые на занятии:
1) Процедура создания ключей алгоритма RSA.
2) Процедура шифрования по алгоритму RSA.

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 15-16

Тема: Шифрование с открытым ключом. Алгоритм на основе задачи об укладке ранца
Основные вопросы, рассматриваемые на занятии:
1) Процедура создания ключей.
2) Процедура шифрования.
3) Процедура расшифрования.

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 17-18

Тема: Шифрование с открытым ключом. Алгоритм шифрования Эль-Гамаля
Основные вопросы, рассматриваемые на занятии:
1) Процедура создания ключей.
2) Процедура шифрования.
3) Процедура расшифрования.

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 19-20

Тема: Оценка стойкости парольной защиты
Основные вопросы, рассматриваемые на занятии:
1) Стойкость подсистемы идентификации и аутентификации.
2) Количественная оценка стойкости парольной защиты.

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 21-22

Тема: Управление криптоключами.

Основные вопросы, рассматриваемые на занятии:
1) Алгоритм генерации простого числа.
2) Алгоритм обмена ключами по схеме Диффи-Хеллмана.

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ № 23-24

Тема: Программирование протоколов аутентификации пользователей.
Основные вопросы, рассматриваемые на занятии:
1) Аутентификация на основе многоразовых паролей.
2) Аутентификация на основе одноразовых паролей.

5.3. Примерная тематика курсовых работ

Учебным планом не предусмотрены

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
ОПК-3					
Базовый	**Знать:** базовые понятия информатики и ИКТ, используемые в области защиты информации и обеспечения информационной безопасности;	Не знает базовые понятия информатики и ИКТ, используемые в области защиты информации и обеспечения информационной безопасности;	В целом знает базовые понятия информатики и ИКТ, используемые в области защиты информации и обеспечения информационной безопасности;	Знает базовые понятия информатики и ИКТ, используемые в области защиты информации и обеспечения информационной безопасности;	

	Современное состояние и тенденции развития методов и организационно-правовое обеспечение информационной безопасности; технологии эффективной защиты информации и информационной безопасности.	Современное состояние и тенденции развития методов и организационно-правовое обеспечение информационной безопасности; технологии эффективной защиты информации и информационной безопасности.	Современное состояние и тенденции развития методов и организационно-правовое обеспечение информационной безопасности; технологии эффективной защиты информации и информационной безопасности.	Современное состояние и тенденции развития методов и организационно-правовое обеспечение информационной безопасности; технологии эффективной защиты информации и информационной безопасности.	
	Уметь: классифицировать угрозы информационной безопасности объекта.	Не умеет классифицировать угрозы информационной безопасности объекта.	В целом умеет классифицировать угрозы информационной безопасности объекта.	Умеет реализовывать классифицировать угрозы информационной безопасности объекта.	
	Владеть: основными методами защиты информации; практическими навыками организации защиты информации и обеспечения информационной безопасности.	Не владеет основными методами защиты информации; практическими навыками организации защиты информации и обеспечения информационной безопасности.	В целом владеет основными методами защиты информации; практическими навыками организации защиты информации и обеспечения информационной безопасности.	Владеет основными методами защиты информации; практическими навыками организации защиты информации и обеспечения информационной безопасности.	
Повышенный	**Знать:** Базовые понятия информатики и ИКТ, используемые в области защиты информации и обеспечения информационной безопасности; Современное состояние и тенденции развития методов и организационно-правовое обеспечение информационной безопасности; технологии эффективной защиты информации и				В полном объеме знает базовые понятия информатики и ИКТ, используемые в области защиты информации и обеспечения информационной безопасности; Современное состояние и тенденции развития методов и организационно-правовое обеспечение информационной безопасности; технологии эффективной защиты

	информационной безопасности.				информации и информационной безопасности.
	Уметь: классифицировать угрозы информационной безопасности объекта.				Умеет в полном объеме классифицировать угрозы информационной безопасности объекта.
	Владеть: основными методами защиты информации; практическими навыками организации защиты информации и обеспечения информационной безопасности.				В полном объеме владеет основными методами защиты информации; практическими навыками организации защиты информации и обеспечения информационной безопасности.
ОПК-5					
Базовый	**Знать:** основные принципы аппаратно-программной защиты информации.	Не знает основные принципы аппаратно-программной защиты информации.	В целом знает основные принципы аппаратно-программной защиты информации.	Знает особенности работы над сбором, проверкой и анализом информации	
	Уметь: реагировать на различные угрозы информационной безопасности.	Не умеет реагировать на различные угрозы информационной безопасности.	В целом умеет реагировать на различные угрозы информационной безопасности.	Умеет выбирать реагировать на различные угрозы информационной безопасности.	
	Владеть: навыками применения и настройки антивирусных систем и систем распознавания угроз и атак.	Не владеет навыками применения и настройки антивирусных систем и систем распознавания угроз и атак.	В целом владеет навыками применения и настройки антивирусных систем и систем распознавания угроз и атак.	Владеет навыками применения и настройки антивирусных систем и систем распознавания угроз и атак.	
Повышенный	**Знать:** основные принципы аппаратно-программной защиты информации.				В полном объеме знает основные принципы аппаратно-программной защиты информации.
	Уметь: реагировать на различные угрозы информационной				В полном объеме умеет реагировать на различные угрозы информационной

	безопасности.				безопасности.
	Владеть: навыками применения и настройки антивирусных систем и систем распознавания угроз и атак.				В полном объеме владеет навыками применения и настройки антивирусных систем и систем распознавания угроз и атак.

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

7.2.1. Типовые темы к письменным работам, докладам и выступлениям:

1. Составляющие информационной безопасности.
2. История криптографии.
3. Методы реализации угроз информационной безопасности.
4. Законодательные акты РФ в области информационной безопасности и защиты информации.
5. Информационная война.
6. Основные требования к шифрам.
7. Алгоритмы хэширования.
8. Факторы, определяющие качество антивирусных программ.
9. Основные функции подсистемы защиты операционной системы.
10. Технологии межсетевых экранов.

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.

7.2.2. Примерные вопросы к итоговой аттестации (экзамен)

1) Понятия «информационная безопасность» и «защита информации». Составляющие информационной безопасности (доступность, целостность и конфиденциальность информации).
2) Уровни формирования режима информационной безопасности (законодательно-правовой, административный (организационный) и программно-технический).
3) Административный уровень обеспечения информационной безопасности: цели и содержание.
4) Классификация угроз информационной безопасности (по составляющим информационной безопасности, по компонентам информационных систем, по характеру воздействия, по расположению источника угроз).
5) Анализ угроз информационной безопасности (угрозы нарушения доступности, целостности и конфиденциальности информации).
6) Модель угроз и модель нарушителя информационной безопасности.
7) Правовые основы информационной безопасности общества (акты федерального законодательства, нормативно-методические документы, стандарты информационной безопасности).
8) Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации (Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»; Закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).
9) Ответственность за нарушения в сфере информационной безопасности.
10) Стандарты информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
11) Общедоступная информация. Информация ограниченного доступа (государственная тайна, конфиденциальная информация).
12) Виды конфиденциальной информации (персональные данные; тайна следствия и судопроизводства; служебная тайна; профессиональная тайна; коммерческая тайна; сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них; сведения об осужденных).
13) Защита интеллектуальной собственности средствами патентного и авторского права.
14) Основные понятия криптографической защиты информации (шифр, зашифровывание, расшифровывание, ключ шифрования, классы криптосистем).
15) Симметричные криптосистемы шифрования. Имитовставка.
16) Асимметричные криптосистемы шифрования. Открытый ключ, секретный ключ.
17) Комбинированная криптосистема шифрования.
18) Управление криптоключами. Метод открытого распределения ключей Диффи – Хеллмана.
19) Классификация криптографических алгоритмов (бесключевые, одноключевые и двухключевые алгоритмы; блочное и поточное шифрование; электронная цифровая подпись).
20) Симметричные алгоритмы шифрования. Блочные алгоритмы шифрования данных (Алгоритм шифрования данных DES).
21) Асимметричные криптоалгоритмы.
22) Назначение электронной цифровой подписи.
23) Процедуры цифровой подписи.
24) Функция хэширования.
25) Вредоносные программы как угроза информационной безопасности. Функции вредоносных программ.

26) Классификация вредоносного программного обеспечения (сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты).
27) Методы обнаружения вредоносных программ (сканирование, обнаружение изменений, эвристический анализ, резидентные сторожа, вакцинирование).
28) Антивирусные программы. Факторы, определяющие качество антивирусных программ.
29) Защита от несанкционированного доступа в компьютерных системах
30) Идентификация и аутентификация пользователей и программ
31) Методы аутентификации, использующие пароли и PIN-коды
32) Угрозы безопасности операционной системы.
33) Понятие защищенной операционной системы.
34) Основные функции подсистемы защиты операционной системы.
35) Разграничение доступа к объектам операционной системы.
36) Обеспечение информационной безопасности компьютерных сетей.
37) Функции межсетевого экрана.
38) Особенности функционирования межсетевого экрана на различных уровнях модели OSI.
39) Схемы сетевой защиты на базе межсетевого экрана.
40) Инженерная защиты объекта информатизации.
41) Техническая охрана объекта информатизации.

Критерии оценки устного ответа на вопросы по дисциплине «Защита информации»:

✓ 5 баллов - 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.

✓ 4 - балла - 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.

✓ 3 балла – 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.

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

7.2.3. Тестовые задания для проверки знаний студентов

1. (ОПК-3)

Защита информации – это..

- ☐ **комплекс мероприятий, направленных на обеспечение информационной безопасности**
- ☐ процесс сбора, накопления, обработки, хранения, распределения и поиска

информации
- ☐ процесс разработки структуры базы данных в соответствии с требованиями пользователей
- ☐ небольшая программа для выполнения определенной задачи

2. (ОПК-3)

Какой термин определяет защищенность информации, ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений — производителям, владельцам и пользователям информации и поддерживающей инфраструктуре?

- ☐ стратегическая безопасность
- ☐ **информационная безопасность**
- ☐ экономическая безопасность
- ☐ корпоративная безопасность

3. (ОПК-3)

Гарантия получения требуемой информации или информационной услуги пользователем за определенное время называется …

- ☐ целостностью
- ☐ **доступностью**
- ☐ конфиденциальностью

4. (ОПК-3)

Гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена называется …

- ☐ целостностью
- ☐ доступностью
- ☐ **конфиденциальностью**

5. (ОПК-3)

Какой аспект информационной безопасности отражает актуальность и непротиворечивость информации, её защищенность от разрушения и несанкционированного изменения?

- ☐ **целостность**
- ☐ конфиденциальность
- ☐ доступность

6. (ОПК-3)

Если злоумышленник подменил исходное сообщение, передаваемое по сети Интернет, какое свойство информации он нарушил?

- ☐ **целостность**
- ☐ конфиденциальность
- ☐ доступность

7. (ОПК-3)

Если в результате DoS-атаки злоумышленников сайт перестал работать, какой аспект информационной безопасности был нарушен?

- ☐ целостность

- ☐ конфиденциальность
- ☐ **доступность**

8. (ОПК-3)

Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?

- ☐ атака
- ☐ **угроза**
- ☐ уязвимость
- ☐ слабое место системы

9. (ОПК-3)

Кто такой инсайдер?

- ☐ **сотрудник, являющийся источником утечки информации**
- ☐ любой источник утечки информации
- ☐ программа-вирус являющаяся источником утечки информации

10. (ОПК-3)

Как называется модель, описывающая вероятный облик злоумышленника, т. е. его квалификацию, имеющиеся средства для реализации тех или иных атак, обычное время действия и т. п?

- ☐ модель угрозы
- ☐ модель уязвимости
- ☐ **модель нарушителя**
- ☐ модель безопасности

11. (ОПК-3)

Какой уровень защиты информации представляет собой комплекс мер, применяемых руководством организации?

- ☐ законодательный
- ☐ процедурный
- ☐ программно-технический
- ☐ **административный**

12. (ОПК-3)

К какому уровню обеспечения ИБ относится «Доктрина информационной безопасности Российской Федерации»?

- ☐ **законодательный**
- ☐ административный
- ☐ процедурный
- ☐ научно-технический

13. (ОПК-3)

В каком законе РФ прописано индивидуальные право каждого гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом?

- ☐ закон «О персональных данных»
- ☐ закон «Об электронной подписи»

- ☐ **Конституция РФ**
- ☐ Доктрина информационной безопасности

14. (ОПК-3)

К какой категории охраняемой информации относится врачебная тайна?

- ☐ государственная тайна
- ☐ служебная тайна
- ☐ **профессиональная тайна**
- ☐ объекты авторского права

15. (ОПК-3)

Какой из законов РФ назначает уголовную ответственность за неправомерный доступ к компьютерной информации?

- ☐ **Уголовный кодекс РФ**
- ☐ Гражданский кодекс РФ
- ☐ Конституция РФ
- ☐ Доктрина информационной безопасности

16. (ОПК-5)

Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?

- ☐ асимметричный
- ☐ **симметричный**
- ☐ правильного ответа нет

17. (ОПК-5)

Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется:

- ☐ шифрование
- ☐ дешифровка
- ☐ **расшифровка**

18. (ОПК-5)

В каких основных форматах существует симметричный алгоритм?

- ☐ блока и строки;
- ☐ **потока и блока;**
- ☐ потока и данных

19. (ОПК-5)

Открытым текстом в криптографии называют:

- ☐ расшифрованный текст
- ☐ любое послание
- ☐ **исходное послание**

20. (ОПК-5)

Какой ключ известен только приемнику?

- ☐ открытый
- ☐ **закрытый**

21. (ОПК-5)

Наука, занимающаяся защитой информации, путем преобразования этой информации это:

- ☐ криптография
- ☐ **криптология**
- ☐ криптоанализ

22. (ОПК-5)

В каких **шифрах результат шифрования очередного блока зависит только от** него самого и не зависит от других блоков шифруемого массива данных?

- ☐ в потоковых
- ☐ **в блочных**

23. (ОПК-5)

Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:

- ☐ шифр функциональных преобразований
- ☐ шифр замен
- ☐ **шифр перестановок**

24. (ОПК-5)

Шифрование-это:

- ☐ процесс создания алгоритмов шифрования
- ☐ процесс сжатия информации
- ☐ **процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется**

25. (ОПК-5)

Стойкость ключа характеризуется

- ☐ длинной
- ☐ непредсказуемостью
- ☐ **все варианты правильные**
- ☐ правильного варианта нет

26. (ОПК-5)

В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией?

- ☐ **при шифровании с помощью ассимметричного алгоритма**
- ☐ при шифровании с помощью симметричного алгоритма
- ☐ арбитр необходим всегда

27. (ОПК-5)

Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый?

- ☐ **нет**
- ☐ да
- ☐ в редких случаях

28. (ОПК-5)

Аутентификацией называют:

- ☐ процесс регистрации в системе
- ☐ способ защиты системы
- ☐ **процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов**

29. (ОПК-5)

Атака – это…

- ☐ **попытка реализации угрозы**
- ☐ потенциальная возможность определенным образом нарушить информационную безопасность
- ☐ программы, предназначенные для поиска необходимых программ

30. (ОПК-5)

Наличие межсетевого экрана необходимо при?

- ☐ использовании автономного автоматизированного рабочего места
- ☐ **использовании сетей общего пользования**
- ☐ использовании изолированной локальной сети

Методические материалы, определяющие процедуры оценивания знаний

1) 1
2) 2
3) 2
4) 3
5) 1
6) 1
7) 3
8) 2
9) 1
10) 3
11) 4
12) 1
13) 2
14) 3
15) 1
16) 2
17) 3
18) 2
19) 3
20) 2
21) 2
22) 2
23) 3
24) 3
25) 3
26) 1
27) 1
28) 3
29) 1
30) 2

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

«неудовлетворительно» – 50% и менее

«удовлетворительно» – 51-80%

«хорошо» – 81-90%

«отлично» – 91-100%

Критерии оценки тестового материала по дисциплине «Защита информации»:

✓ 5 баллов - выставляется студенту, если выполнены все задания варианта, продемонстрировано знание фактического материала (базовых понятий, алгоритма, факта).

✓ 4 балла - работа выполнена вполне квалифицированно в необходимом объёме; имеются незначительные методические недочёты и дидактические ошибки. Продемонстрировано умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; понятен творческий уровень и аргументация собственной точки зрения

✓ 3 балла – продемонстрировано умение синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей в рамках определенного раздела дисциплины;

✓ 2 балла - работа выполнена на неудовлетворительном уровне; не в полном объёме, требует доработки и исправлений, и исправлений более чем половины объема.

7.2.4. Балльно-рейтинговая система оценки знаний бакалавров

Согласно Положения о балльно-рейтинговой системе оценки знаний бакалавров баллы выставляются в соответствующих графах журнала (см. «Журнал учета балльно-рейтинговых показателей студенческой группы») в следующем порядке:

«Посещение» - 2 балла за присутствие на занятии без замечаний со стороны преподавателя; 1 балл за опоздание или иное незначительное нарушение дисциплины; 0 баллов за пропуск одного занятия (вне зависимости от уважительности пропуска) или опоздание более чем на 15 минут или иное нарушение дисциплины.

«Активность» - от 0 до 5 баллов выставляется преподавателем за демонстрацию студентом знаний во время занятия письменно или устно, за подготовку домашнего задания, участие в дискуссии на заданную тему и т.д., то есть за работу на занятии. При этом преподаватель должен опросить не менее 25% из числа студентов, присутствующих на практическом занятии.

«Контрольная работа» или «тестирование» - от 0 до 5 баллов выставляется преподавателем по результатам контрольной работы или тестирования группы, проведенных во внеаудиторное время. Предполагается, что преподаватель по согласованию с деканатом проводит подобные мероприятия по выявлению остаточных знаний студентов не реже одного раза на каждые 36 часов аудиторного времени.

«Отработка» - от 0 до 2 баллов выставляется за отработку каждого пропущенного лекционного занятия и от 0 до 4 баллов может быть поставлено преподавателем за отработку студентом пропуска одного практического занятия или практикума. За один раз можно отработать не более шести пропусков (т.е., студенту выставляется не более 18 баллов, если все пропущенные шесть занятий являлись практическими) вне зависимости от уважительности пропусков занятий.

«Пропуски в часах всего» - количество пропущенных занятий за отчетный период умножается на два (1 занятие=2 часам) (заполняется делопроизводителем деканата).

«Пропуски по неуважительной причине» - графа заполняется делопроизводителем деканата.

«Попуски по уважительной причине» - графа заполняется делопроизводителем деканата.

«Корректировка баллов за пропуски» - графа заполняется делопроизводителем деканата.

«Итого баллов за отчетный период» - сумма всех выставленных баллов за данный период (графа заполняется делопроизводителем деканата).

Таблица перевода балльно-рейтинговых показателей в отметки традиционной системы оценивания

Соотношение часов лекционных и практических занятий	**0/2**	**1/3**	**1/2**	**2/3**	**1/1**	**3/2**	**2/1**	**3/1**	**2/0**	**Соответствие отметки коэффициенту**
Коэффициент соответствия балльных показателей традиционной отметке	1,5	1,1	1,1	1,1	1,1	1,1	1,1	1,1	1,1	«зачтено»
	1	1	1	1	1	1	1	1	1	«удовлетворительно»
	2	1,75	1,65	1,6	1,5	1,4	1,35	1,25	-	«хорошо»
	3	2,5	2,3	2,2	2	1,8	1,7	1,5	-	«отлично»

Необходимое количество баллов для выставления отметок («зачтено», «удовлетворительно», «хорошо», «отлично») определяется произведением реально проведенных аудиторных часов (n) за отчетный период на коэффициент соответствия в зависимости от соотношения часов лекционных и практических занятий согласно приведенной таблице.

«Журнал учета балльно-рейтинговых показателей студенческой группы» заполняется преподавателем на каждом занятии.

В случае болезни или другой уважительной причины отсутствия студента на занятиях, ему предоставляется право отработать занятия по индивидуальному графику.

Студенту, набравшему количество баллов менее определенного порогового уровня, выставляется оценка "неудовлетворительно" или "не зачтено". Порядок ликвидации задолженностей и прохождения дальнейшего обучения регулируется на основе действующего законодательства РФ и локальных актов КЧГУ.

Текущий контроль по лекционному материалу проводит лектор, по практическим занятиям – преподаватель, проводивший эти занятия. Контроль может проводиться и совместно.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины. Информационное обеспечение образовательного процесса

8.1. Основная литература

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013711 (дата обращения: 12.03.2021). – Режим доступа: по подписке.
2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093695 (дата обращения: 12.03.2021). – Режим доступа: по подписке.

3. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - Москва : ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. (Высшее образование: Бакалавриат; Магистратура). ISBN 978-5-369-01378-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/474838 (дата обращения: 12.03.2021). – Режим доступа: по подписке.
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, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 (дата обращения: 28.02.2021). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Баранова, Е. К. Основы информатики и защиты информации : учебное пособие / Е. К. Баранова. - Москва : РИОР : ИНФРА-М, 2013. - 183 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01169-0 (РИОР), ISBN 978-5-16-006484-0 (ИНФРА-М). - Текст : электронный. - URL: https://znanium.com/catalog/product/415501 (дата обращения: 06.03.2021). – Режим доступа: по подписке.
2. Криптографическая защита информации : учебное пособие / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.] ; под ред. С. О. Крамарова. — Москва : РИОР : ИНФРА-М, 2021. — 321 с. — (Высшее образование). - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1153156 (дата обращения: 12.03.2021). – Режим доступа: по подписке.

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.
Лабораторные занятия	Конспектирование источников. Работа с конспектом лекций, выполнение заданий, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом
Контрольная работа/ индивидуальные задания	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.
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 экзамену	При подготовке к экзамену 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
2021 / 2022 учебный годгод	Электронно-библиотечная система ООО «Знаниум». Договор № 5184 ЭБС от 25 марта 2021г.	с 30.03.2021 г по 30.03.2022 г.
	Электронно-библиотечная система «Лань». Договор № СЭБ НВ-294 от 1 декабря 2020 года.	Бессрочный
2021 /2022 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
2021 / 2022 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
2023-2024 уч. год	Электронно-библиотечная система ООО «Знаниум». Договор № 915 ЭБС от 25.05.20231 г.	действия с 25.05.2023 г. по 15.05.2024 г

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.
Учебный корпус № 2, ауд. 16

Лаборатория общей и экспериментальной физики для проведения занятий лабораторного, лекционного, семинарского типов, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций.
Специализированная мебель: столы ученические, стулья, стол преподавателя, доска меловая, учебная и научная литература, таблицы физических констант.
Технические средства обучения: персональный компьютер с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, переносной проектор.
Комплект лабораторных работ и необходимого оборудования для их выполнения по всем разделам общей и экспериментальной физики.
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
- Kaspersky Endpoint Security (Лицензия № 0E26-190214-143423-910-82), с 14.02.2019 по 02.03.2021г.
- Kaspersky Endpoint Security (Лицензия № 280E-210210-093403-420-2061), с 03.03.2021 по 04.03.2023г.
- Антивирус Касперского. Действует до 03.03.2025 г (договор № 56/2023 от 25 января 2023г.);

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

1. Аудитория для самостоятельной работы студентов.

Специализированная мебель:
столы ученические, стулья, доска маркерная.
Учебно-наглядные пособия (в электронном виде).
Технические средства обучения:
Персональные компьютеры в количестве 20 шт. с подключением к информационно-телекоммуникационной 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
- Kaspersky Endpoint Security (Лицензия № 0E26-190214-143423-910-82), с 14.02.2019 по 02.03.2021г.
- Kaspersky Endpoint Security (Лицензия № 280E-210210-093403-420-2061), с 03.03.2021 по 04.03.2023г.
- пакет приложений для объектно-ориентированного программирования Embarcadero (Item Number: 2013123054325206. Срок действия лицензии: бессрочная);
- пакет визуального редактирования растровых изображений GIMP (Лицензия № GNU GPLv3. Срок действия лицензии: бессрочная);

- образовательная подписка Google G Suite for Education (видеоконференции, дневник, календарь, диск и прочее). (Срок действия лицензии: бессрочная);
- пакет математического моделирования Mathcad (Contract Number (SCN) 4A1913127. Срок действия лицензии: бессрочная);
- подписка на программные продукты Microsoft «Azure Dev Tools for Teaching» (Идентификатор подписчика: ICM-166172). С 2019 г. по 2021 г.;
- система поиска заимствований в текстах «Антиплагиат ВУЗ» (Договор № 3262 от 20.01.2021 г.);
- Информационно-правовая система «Инофрмио» (Договор № НК 1017 от 20.01.2021 г.);
- пакет визуального 3D-моделтрования Blender (Лицензия № GNU GPL v3. Срок действия лицензии: бессрочная);
- векторный графический редактор Inkscape (Лицензия № GNU GPL v3. Срок действия лицензии: бессрочная);
- программный комплекс для верстки Scribus (Лицензия № GNU GPL v3. Срок действия лицензии: бессрочная);
- Autodesk AutoCAD (Лицензия № 5X6-30X999XX. Бессрочная образовательная (академическая) лицензия);
- Autodesk 3DS Max (Лицензия № 5X5-93X928XX. Бессрочная образовательная (академическая) лицензия);
- Autodesk Revit (Лицензия № 5X6-03X109XX. Бессрочная образовательная (академическая) лицензия).
- Антивирус Касперского. Действует до 03.03.2025 г (договор № 56/2023 от 25 января 2023г.);

(369200, Карачаево-Черкесская республика, г. Карачаевск, ул. Ленина, 29, учебно-лабораторный корпус, ауд. 507)

2. Научный зал, 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
- Kaspersky Endpoint Security (Лицензия № 0E26-190214-143423-910-82), с 14.02.2019 по 02.03.2021г.
- Kaspersky Endpoint Security (Лицензия № 280E-210210-093403-420-2061), с 03.03.2021 по 04.03.2023г
- Антивирус Касперского. Действует до 03.03.2025 г (договор № 56/2023 от 25 января 2023г.);

(369200, Карачаево-Черкесская республика, г. Карачаевск, ул. Ленина, 29. Учебно-лабораторный корпус, каб.101)

3. Читальный зал, 80 мест, 10 компьютеров.

Специализированная мебель: столы ученические, стулья.

Технические средства обучения:

Дисплей Брайля ALVA с программой экранного увеличителя MAGic Pro;

стационарный видеоувеличитель 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 Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная
- Google G Suite for Education (IC: 01i1p5u8), бессрочная
- Kaspersky Endpoint Security (Лицензия № 0E26-190214-143423-910-82), с 14.02.2019 по 02.03.2021г.
- Kaspersky Endpoint Security (Лицензия № 280E-210210-093403-420-2061), с 03.03.2021 по 04.03.2023г.
- Антивирус Касперского. Действует до 03.03.2025 г (договор № 56/2023 от 25 января 2023г.);

(369200, Карачаево-Черкесская республика, г. Карачаевск, ул. Ленина, 29. Учебно-лабораторный корпус, каб.102а)

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. GNU Image Manipulation Program (GIMP) (лицензия: №GNU GPLv3), бессрочная.
4. Google G Suite for Education (IC: 01i1p5u8), бессрочная.
5. Kaspersky Endpoint Security (OE26-190214-143423-910-82), с 14.02.2019 по 02.03.2021 г.
6. Kaspersky Endpoint Security (лицензия №280E2102100934034202061), с 03.03.2021 по 04.03.2023 г.
7. Microsoft Office (лицензия №60127446), бессрочная.
8. Microsoft Windows (лицензия №60290784), бессрочная
9. Антивирус Касперского. Действует до 03.03.2025 г (договор № 56/2023 от 25 января 2023г.);

10.4. Современные профессиональные базы данных и информационные справочные системы

Современные профессиональные базы данных

1. Банк данных угроз безопасности информации. ФСТЭК России - https://bdu.fstec.ru/threat

2. Федеральный портал «Российское образование» - https://edu.ru/documents/

3. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) – http://school-collection.edu.ru/

4. 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.

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 процессе овладения обучающимися с ОВЗ компетенциями, предусмотренными рабочей программой дисциплины преподаватель руководствуется следующими принципами построения инклюзивного образовательного пространства:

– Принцип индивидуального подхода, предполагающий выбор форм, технологий, методов и средств обучения и воспитания с учетом индивидуальных образовательных потребностей каждого из обучающихся с ОВЗ, учитывающими различные стартовые возможности данной категории обучающихся (структуру, тяжесть, сложность дефектов развития).

– Принцип вариативной развивающей среды, который предполагает наличие в процессе проведения учебных занятий и самостоятельной работы обучающихся необходимых развивающих и дидактических пособий, средств обучения, а также организацию безбарьерной среды, с учетом структуры нарушения в развитии (нарушения опорно-двигательного аппарата, зрения, слуха и др.).

– Принцип вариативной методической базы, предполагающий возможность и способность использования преподавателем в процессе овладения обучающимися с ОВЗ

данной учебной дисциплиной, технологий, методов и средств работы из смежных областей, применение методик и приемов тифло-, сурдо-, логопедии.

– Принцип самостоятельной активности обучающихся с ОВЗ, предполагающий обеспечение самостоятельной познавательной активности данной категории обучающихся посредством дополнения раздела РПД «Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине» заданиями, учитывающими различные стартовые возможности данной категории обучающихся (структуру, тяжесть, сложность дефектов развития).

В группах, в состав которых входят обучающиеся с ОВЗ, в процессе проведения учебных занятий осуществляется учет наиболее типичных проявлений психоэмоционального развития, поведенческих особенностей, свойственных обучающимся с ОВЗ: повышенной утомляемости, инертности эмоциональных реакций, нарушений психомоторной сферы, недостаточное развитие вербальных и невербальных форм коммуникации. В отдельных случаях учитывается их склонность к перепадам настроения, аффективность поведения, повышенный уровень тревожности, склонность к проявлениям агрессии, негативизма.

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;
- видеокомплекты 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, видеоувеличителем, клавиатурой для лиц с ДЦП, роллером Распределение специализированного оборудования.

12. Лист регистрации изменений

Изменение	Дата и номер 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. На антивирус Касперского. (Договор №56/2023 от 25 января 2023г.). Действует до 03.03.2025г. 2.Договор № 238 ЭБС ООО «Знаниум» от 23.04.2024г. Действует до 26.05.2025г. 3.Договор № 36 от 14.03.2024г. эбс «Лань». Действует по 19.01.2025г. 4.Договор № 25 эбс «ЮРАЙТ» от 28.05.2024г. Действует до 11 мая 2025г.		29.05.2024г., протокол № 8	30.05.2024г.,