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
«30» апреля 2025 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) программы:

Программное обеспечение средств вычислительной техники и автоматизированных систем

Квалификация выпускника

бакалавр

Форма обучения

Очная

Год начала подготовки - **2025**

Карачаевск, 2025

Составитель: д-р физ.-мат. наук, доцент Узденова А.М.

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 №929 с изменениями и дополнениями от 26.11.2020 г. №1456, от 8.02.2021 г. №83, на основании учебного плана подготовки бакалавров по направлению 09.03.01 Информатика и вычислительная техника, профиль – Программное обеспечение средств вычислительной техники и автоматизированных систем, локальных актов КЧГУ.

Рабочая программа рассмотрена и утверждена на заседании кафедры информатики и вычислительной математики на 2025-2026 учебный год, протокол №8 от 25 апреля 2025 г.

Оглавление

1. Наименование дисциплины (модуля):

Защита информации

Целью изучения дисциплины является формирование у бакалавров общепрофессиональных компетенций путем 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:

- изучить методы и средства обеспечения защиты информации
- изучить необходимый понятийный аппарат дисциплины;
- сформировать умение проводить анализ угроз безопасности;
- сформировать навыки использования методов и средств защиты информации.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.О.10 «Защита информации» относится к блоку – «Блок 1. Обязательная часть».

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

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПВО	
Индекс	Б1.О.10
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/ОПВО	Индикаторы достижения сформированности компетенций
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 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.
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 ИС. ОПК-5.3. Владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем.

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 часов.

Объём дисциплины	**Всего часов**		
	Очная форма обучения	**Очно-заочная форма обучения**	**Заочная форма 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			
практикумы			
лабораторные работы	48		
Внеаудиторная работа:			
консультация перед экзаменом			
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)

Очная форма обучения

№ п/п	Курс/семестр	Раздел, тема дисциплины	Общая трудоемкость (в часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
			Всего	Аудиторные уч. занятия			Сам. работа
			180	Лек.	Пр.	Лаб.	
	4/8	**Раздел 1. Общие положения информационной безопасности**	**30**	**4**		**8**	**18**
1.		Проблемы обеспечения информационной безопасности	2	2			
2.		Составляющие информационной безопасности	3				3
3.		Основы шифрования данных.	4			4	
4.		История криптографии	6				6
5.		Угрозы информационной безопасности	2	2			
6.		Методы реализации угроз информационной безопасности	3				3
7.		Использование шифров замены для защиты информации	4			4	
8.		Шифры однозначной замены. Полиграммные шифры	6				6
		Раздел 2. Нормативно-правовое обеспечение информационной безопасности	**30**	**4**		**8**	**18**
9.		Нормативно-правовые основы информационной безопасности в РФ	2	2			
10.		Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации	3				3
11.		Шифры замены	4			4	
12.		Омофонические шифры	6				6
13.		Основные виды «конфиденциальной» информации	2	2			
14.		Информационная война	3				3
15.		Шифры перестановки	4			4	
16.		Шифры множественной перестановки	6				6
		Раздел 3. Криптографическая защита информации	**45**	**6**		**12**	**27**
17.		Принципы криптографической защиты информации	2	2			

18.		Тема: Основные требования к шифрам	3				3
19.		Аддитивные шифры	4			4	
20.		Аддитивное шифрование по модулю N	6				6
21.		Криптографические алгоритмы	2	2			
22.		Шифры замены, перестановок, гаммирования, аналитические преобразования и композиционные	3				3
23.		Комбинированные шифры	4			4	
24.		Режимы алгоритма DES	6				6
25.		Электронная цифровая подпись	2	2			
26.		Алгоритмы хэширования	3				3
27.		Шифрование с открытым ключом. Алгоритм RSA	4			4	
28.		Алгоритм RSA	6				6
		Раздел 4. Программно-аппаратная защита информации	**75**	**10**		**20**	**45**
29.		Вредоносные программы и защита от них	2	2			
30.		Факторы, определяющие качество антивирусных программ	3				3
31.		Шифрование с открытым ключом. Алгоритм на основе задачи об укладке ранца	4			4	
32.		Алгоритм на основе задачи об укладке ранца	6				6
33.		Механизмы обеспечения информационной безопасности в информационных системах	2	2			
34.		Аутентификация на основе многоразовых и одноразовых паролей	3				3
35.		Шифрование с открытым ключом. Алгоритм шифрования Эль-Гамаля	4			4	
36.		Алгоритм шифрования Эль-Гамаля	6				6
37.		Обеспечение информационной безопасности операционных систем	2	2			
38.		Основные функции подсистемы защиты операционной системы	3				3
39.		Оценка стойкости парольной защиты	4			4	
40.		Количественная оценка стойкости парольной защиты	6				6
41.		Методы и средства защиты информации в сети Интернет	2	2			
42.		Технологии межсетевых экранов	3				3
43.		Управление криптоключами	4			4	
44.		Алгоритм обмена ключами по схеме Диффи-Хеллмана	6				6
45.		Инженерно-техническая защита информации	2	2			
46.		Организация режима секретности	3				3
47.		Программирование протоколов аутентификации пользователей	4			4	
48.		Одноразовые и многоразовые пароли	6				6
		Всего	**180**	**24**		**48**	**108**

6. Основные формы учебной работы и образовательные технологии, используемые при реализации образовательной программы

Лекционные занятия. Лекция является основной формой учебной работы в вузе, она является наиболее важным средством теоретической подготовки обучающихся. На лекциях рекомендуется деятельность обучающегося в форме активного слушания, т.е. предполагается возможность задавать вопросы на уточнение понимания темы и рекомендуется конспектирование основных положений лекции. Основная дидактическая цель лекции - обеспечение ориентировочной основы для дальнейшего усвоения учебного материала. Лекторами активно используются: лекция-диалог, лекция - визуализация, лекция - презентация. Лекция - беседа, или «диалог с аудиторией», представляет собой непосредственный контакт преподавателя с аудиторией. Ее преимущество состоит в том, что она позволяет привлекать внимание слушателей к наиболее важным вопросам темы, определять содержание и темп изложения учебного материала с учетом особенностей аудитории. Участие обучающихся в лекции – беседе обеспечивается вопросами к аудитории, которые могут быть как элементарными, так и проблемными.

Главной задачей каждой лекции является раскрытие сущности темы и анализ ее основных положений. Рекомендуется на первой лекции довести до внимания студентов структуру дисциплины и его разделы, а в дальнейшем указывать начало каждого раздела (модуля), суть и его задачи, а, закончив изложение, подводить итог по этому разделу, чтобы связать его со следующим. Содержание лекций определяется настоящей рабочей программой дисциплины. Для эффективного проведения лекционного занятия рекомендуется соблюдать последовательность ее основных этапов:

1. формулировку темы лекции;
2. указание основных изучаемых разделов или вопросов и предполагаемых затрат времени на их изложение;
3. изложение вводной части;
4. изложение основной части лекции;
5. краткие выводы по каждому из вопросов;
6. заключение;
7. рекомендации литературных источников по излагаемым вопросам.

Практические занятия. Дисциплины, по которым планируются практические занятия, определяются учебными планами. Практические занятия относятся к основным видам учебных занятий и составляют важную часть теоретической и профессиональной практической подготовки. Выполнение студентом практических занятий направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплин математического и общего естественно-научного, общепрофессионального и профессионального циклов;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива. Методические рекомендации разработаны с целью единого подхода к организации и проведению практических занятий.

Практическое занятие — это форма организации учебного процесса, направленная на выработку у студентов практических умений для изучения последующих дисциплин (модулей) и для решения профессиональных задач. Практическое занятие должно проводиться в учебных кабинетах или специально оборудованных помещениях. Необходимыми структурными элементами практического занятия, помимо самостоятельной деятельности студентов, являются анализ и оценка выполненных работ и

степени овладения студентами запланированными умениями. Дидактические цели практических занятий: формирование умений (аналитических, проектировочных, конструктивных), необходимых для изучения последующих дисциплин (модулей) и для будущей профессиональной деятельности.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

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 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.

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

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

7.1. Индикаторы оценивания сформированности компетенций

Компетенции	**Зачтено**			**Не зачтено**
	Высокий уровень (отлично) (86-100% баллов)	Средний уровень (хорошо) (71-85% баллов)	Низкий уровень (удовлетворительно) (56-70% баллов)	Ниже порогового уровня (неудовлетворительно) (до 55% баллов)
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с	ОПК-3.1 Полностью знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с	ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением	ОПК-3.1 В целом знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с	ОПК-3.1 Знает фрагментарно 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 безопасности.	применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ОПК-3.2 Полностью 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-3.2 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-3.2 В целом 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-3.2 Не 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 Полностью владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом 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.	ОПК-3.3 Владеет основными навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	ОПК-3.3 Не владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ОПК-5: Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем.	ОПК-5.1 Полностью знает основы системного администрирования, администрирования СУБД, современные стандарты.	ОПК-5.1 Знает основы системного администрирования, администрирования СУБД, современные стандарты.	ОПК-5.1 В целом знает основы системного администрирования, администрирования СУБД, современные стандарты.	ОПК-5.1 Знает фрагментарно основы системного администрирования, администрирования СУБД, современные стандарты.
	ОПК-5.2 Полностью умеет выполнять параметрическую настройку ИС.	ОПК-5.2 Умеет выполнять параметрическую настройку ИС.	ОПК-5.2 В целом умеет выполнять параметрическую настройку ИС.	ОПК-5.2 Не умеет выполнять параметрическую настройку ИС.
	ОПК-5.3 Полностью владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем.	ОПК-5.3 Владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем.	ОПК-5.3 Владеет основными обеспечения по навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем.	ОПК-5.3 Не владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем.

7.2. Перевод балльно-рейтинговых показателей оценки качества подготовки обучающихся в отметки традиционной системы оценивания

Порядок функционирования внутренней системы оценки качества подготовки обучающихся и перевод балльно-рейтинговых показателей обучающихся в отметки традиционной системы оценивания проводится в соответствии с положением КЧГУ «Положение о балльно-рейтинговой системе оценки знаний обучающихся», размещенным на сайте Университета по адресу: https://kchgu.ru/inye-lokalnye-akty/

7.3. Типовые контрольные вопросы и задания, необходимые для оценивания сформированности компетенций в процессе освоения учебной дисциплины

7.3.1. Перечень вопросов для экзамена

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.

7.3.2. 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.

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

8.1. Основная литература

1. 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, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642. – Режим доступа: по подписке.

2. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2140566. – Режим доступа: по подписке.

3. 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, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1899016. – Режим доступа: по подписке.

4. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912987. – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Защита интеллектуальной собственности : учебник для бакалавров / под ред. проф. И. К. Ларионова, доц. М. А. Гуреевой, проф. В. В. Овчинникова. - 5-е изд., стер. - Москва : Издательско-торговая корпорация «Дашков и К°», 2023. - 256 с. - ISBN 978-5-394-05367-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/2082673. – Режим доступа: по подписке.

2. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139841. – Режим доступа: по подписке.

3. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598. – Режим доступа: по подписке.

4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022. – Режим доступа: по подписке.

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

9.1. Общесистемные требования

Электронная информационно-образовательная среда ФГБОУ ВО «КЧГУ»

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) Университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории Университета, так и вне ее.

Функционирование ЭИОС обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее

использующих и поддерживающих. Функционирование ЭИОС соответствует законодательству Российской Федерации.

Адрес официального сайта университета: http://kchgu.ru.

Адрес размещения ЭИОС ФГБОУ ВО «КЧГУ»: https://do.kchgu.ru.

Электронно-библиотечные системы (электронные библиотеки)

Учебный год	Наименование документа с указанием реквизитов	Срок действия документа
2025-2026 учебный год	Электронно-библиотечная система ООО «Знаниум». Договор № 249 эбс от 14.05.2025 г. Электронный адрес: https://znanium.com	от 14.05.2025 г. до 14.05.2026 г.
2025-2026 учебный год	Электронно-библиотечная система «Лань». Договор № 10 от 11.02.2025 г. Электронный адрес: https://e.lanbook.com	от 11.02.2025 г. до 11.02.2026 г.
2025-2026 учебный год	Электронно-библиотечная система КЧГУ. Положение об ЭБ утверждено Ученым советом от 30.09.2015г. Протокол № 1. Электронный адрес: http://lib.kchgu.ru	Бессрочный
2025-2026 учебный год	Национальная электронная библиотека (НЭБ). Договор №101/НЭБ/1391-п от 22.02.2023 г. Электронный адрес: http://rusneb.ru	Бессрочный
2025-2026 учебный год	Научная электронная библиотека «ELIBRARY.RU». Лицензионное соглашение №15646 от 21.10.2016 г. Электронный адрес: http://elibrary.ru	Бессрочный
2025-2026 учебный год	Электронный ресурс Polpred.com Обзор СМИ. Соглашение. Бесплатно. Электронный адрес: http://polpred.com	Бессрочный

9.2. Материально-техническое и учебно-методическое обеспечение дисциплины

Занятия проводятся в учебных аудиториях, предназначенных для проведения занятий лекционного и практического типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации в соответствии с расписанием занятий по образовательной программе. С описанием оснащенности аудиторий можно ознакомиться на сайте университета, в разделе материально-технического обеспечения и оснащенности образовательного процесса по адресу: https://kchgu.ru/sveden/objects/

9.3. Необходимый комплект лицензионного программного обеспечения

- MicrosoftWindows (Лицензия № 60290784), бессрочная;
- MicrosoftOffice (Лицензия № 60127446), бессрочная;
- ABBY FineReader (лицензия № FCRP-1100-1002-3937), бессрочная;
- CalculateLinux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная;
- Google G Suite for Education (IC: 01i1p5u8), бессрочная;
- Kaspersky Endpoint Security (Лицензия № 280E-210210-093403-420-2061), с 25.01.2023 г. по 03.03.2025 г.;
- Kaspersky Endpoint Security. Договор №0379400000325000001/1 от 28.02.2025 г. Срок действия лицензии с 27.02.2025 г. по 07.03.2027 г.

9.4. Современные профессиональные базы данных и информационные справочные системы

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 Elsevirhttp://www.scopus.com/search/form.uri?display=basic.
4. Портал Федеральных государственных образовательных стандартов высшего образования - http://fgosvo.ru.
5. Федеральный центр информационно-образовательных ресурсов (ФЦИОР) – http://edu.ru.
6. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) – http://school-collection.edu.ru.
7. Информационная система «Единое окно доступа к образовательным ресурсам» (ИС «Единое окно») – http://window/edu.ru.

10. Особенности организации образовательного процесса для лиц с ограниченными возможностями здоровья

В ФГБОУ ВО «Карачаево-Черкесский государственный университет имени У.Д. Алиева» созданы условия для получения высшего образования по образовательным программам обучающихся с ограниченными возможностями здоровья (ОВЗ).

Специальные условия для получения образования по ОПВО обучающимися с ограниченными возможностями здоровья определены «Положением об обучении лиц с ОВЗ в КЧГУ», размещенным на сайте Университета по адресу: http://kchgu.ru.

11. 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 в ОПВО	Дата и номер протокола ученого совета Университета, на котором были утверждены изменения в ОПВО