

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

УТВЕРЖДАЮ
И. о. проректора по УР
М. Х. Чанкаев

«30» апреля 2025г., протокол № 8

Рабочая программа дисциплины

Методы и средства защиты информации

(наименование дисциплины (модуля))

Направление подготовки

44.03.05 Педагогическое образование (с двумя профилями подготовки)

(шифр, название направления)

Направленность (профиль)

Математика; информатика

Квалификация выпускника

бакалавр

Форма обучения

очно-заочная, заочная

Год начала подготовки

2025

Карачаевск, 2025

Составитель: старший преподаватель кафедры ИВМ *Ортобаев А.А.*

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), утвержденным приказом Министерства образования и науки Российской Федерации от 22.02.2018 №125; образовательной программой высшего образования и учебным планом по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), направленность (профиль) «Математика; информатика», составленными с учетом требований Методических рекомендаций по подготовке кадров по программам педагогического бакалавриата на основе единых подходов к их структуре и содержанию («Ядро высшего педагогического образования») (одобрено Коллегией Министерства просвещения Российской Федерации 25 ноября 2021 г.); локальными актами КЧГУ.

Рабочая программа рассмотрена и утверждена на заседании кафедры информатики и вычислительной математики на 2025-2026 учебный год, протокол № 8 от 25.04. 2025г

СОДЕРЖАНИЕ

1. Наименование дисциплины (модуля).....	4
2. Место дисциплины (модуля) в структуре образовательной программы.....	4
3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.....	4
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.....	6
5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....	6
5.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах).....	6
5.2. Тематика лабораторных занятий	12
5.3. Примерная тематика курсовых работ.....	12
6. Основные формы учебной работы и образовательные технологии, используемые при реализации образовательной программы.....	12
7. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю).....	13
7.1. Описание шкал оценивания степени сформированности компетенций.....	13
7.2. Перевод балльно-рейтинговых показателей оценки качества подготовки обучающихся в отметки традиционной системы оценивания	14
7.3. Типовые контрольные задания или иные учебно-методические материалы, необходимые для оценивания степени сформированности компетенций в процессе освоения учебной дисциплины	14
7.2.1. Типовые темы к письменным работам, докладам и выступлениям:	15
7.2.2. Примерные вопросы к итоговой аттестации (зачет).....	15
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины. Информационное обеспечение образовательного процесса.....	16
8.1. Основная литература:	16
8.2. Дополнительная литература:.....	16
9. Требования к условиям реализации рабочей программы дисциплины (модуля)	17
9.1. Общесистемные требования	17
9.2. Материально-техническое и учебно-методическое обеспечение дисциплины	17
9.3. Необходимый комплект лицензионного программного обеспечения	18
9.4. Современные профессиональные базы данных и информационные справочные системы	18
10. Особенности организации образовательного процесса для лиц с ограниченными возможностями здоровья.....	18
11. Лист регистрации изменений.....	19

1. Наименование дисциплины (модуля)

Методы и средства защиты 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:

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

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Методы и средства защиты информации» (Б1.О.08.06) относится к предметно-методическому модулю 2 базовой части Б1.

Дисциплина (модуль) изучается на 3 курсе в 5 семестре.

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО	
Индекс	Б1.О.08.06
Требования к предварительной подготовке обучающегося:	
Учебная дисциплина «Методы и средства защиты информации» является базовой, знакомит обучающихся с общими понятиями информационной безопасности.	
Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Изучение дисциплины «Методы и средства защиты информации» необходимо для успешного освоения дисциплин «Теоретические основы информации», «Численные методы», «Информационные системы», «Методы программирования» и другие.	

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

Процесс изучения дисциплины «Методы и средства защиты 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
УК-2	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Определяет совокупность взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм. УК-2.2. Оценивает вероятные риски и ограничения, определяет ожидаемые результаты решения поставленных	Знать: основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации; содержание основных уровней обеспечения информационной безопасности. Уметь: выполнять анализ требований к системе защиты информации; выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационной системе.

		<p>задач.</p> <p>УК-2.3. Использует инструменты и техники цифрового моделирования для реализации образовательных процессов</p>	<p>Владеть:</p> <p>навыками использования методов организации и контроля функционирования системы защиты информации; навыками использования стандартов для защиты информации в информационной системе.</p>
ОПК-9	<p>ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности</p>	<p>ОПК-9.1. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности</p> <p>ОПК-9.2. Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности</p>	<p>Знать: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации.</p> <p>Уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения.</p> <p>Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.</p>
ПК-1	<p>ПК-1.</p> <p>Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач</p>	<p>ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета)</p> <p>ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО</p> <p>ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные</p>	<p>Знать: структуру, состав и дидактические единицы предметной области (преподаваемого предмета)</p> <p>Уметь: осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО</p> <p>Владеть: умением разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные</p>

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 3 ЗЕТ, 108 академических часа.

Объем дисциплины	Всего часов	
	Для очно-заочной формы обучения	для заочной формы обучения
Общая трудоемкость дисциплины	108	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)	44	
Аудиторная работа (всего):	44	8
лекции	14	2
семинары, практические занятия	30	6
практикумы	Не предусмотрено	Не предусмотрено
лабораторные работы	Не предусмотрено	Не предусмотрено
Внеаудиторная работа:		
консультация перед зачетом		
Самостоятельная работа обучающихся (всего)	28	92
Контроль самостоятельной работы	36	8
Вид промежуточной аттестации обучающегося (зачет / экзамен)	Экзамен-6 семестр	Экзамен- 4 семестр

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 очно-заочной формы обучения

№ п/п	Раздел, тема дисциплины	Общая трудоемкость (в часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)					Формы текущего контроля	
			всего	Аудиторные уч. занятия			Сам. работа		Планируемые результаты обучения
				Лек	Пр	Лаб			
	Раздел 1. Понятие и сущность информационной безопасности и защиты информации.	30	8	6		16			
1	Тема: Необходимость и значимость нормативно-правового определения основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. <i>/лз/</i>	4	2	2			УК-2 ОПК-9 ПК-1	Устный опрос	

2	Защита документов MS Office /пр/	2		2			УК-2 ОПК-9 ПК-1	Отчет по прак.работе
3	Тема: Основные компоненты безопасности государства и доминирующая роль ИБ. Становление и развитие понятия «информационная безопасность». Связь ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации. /ср/	6				6	УК-2 ОПК-9 ПК-1	Вопросы к зачету
4	Тема: Основные угрозы информационной безопасности. Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. /лз/	2	2				УК-2 ОПК-9 ПК-1	Блиц-опрос
5	Тема: Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). /нр/	4		4			УК-2 ОПК-9 ПК-1	Доклад с презентацией
6	Тема: Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз. /ср/	8		2		6	УК-2 ОПК-9 ПК-1	Реферат
	Раздел 2. Основные уровни информационной безопасности.	20	8	4		8	УК-2 ОПК-9 ПК-1	
7	Тема: Правовой и административный уровень обеспечения информационной безопасности /лз/	2	2				УК-2 ОПК-9 ПК-1	Устный опрос
8	Тема: Базовые методы криптографического преобразования данных. /пр/	2		2			УК-2 ОПК-9 ПК-1	Отчет по прак.работе
9	Тема: Программно-технический уровень обеспечения защиты информации /лз/	2	2				УК-2 ОПК-9 ПК-1	Блиц опрос
10	Тема: Использование методов замены для	2		2			УК-2 ОПК-9	Отчет по прак.работе

	шифрования данных. /np/						ПК-1	
11	Тема: Процедурный уровень информационной безопасности /ср/	4				4	УК-2 ОПК-9 ПК-1	Вопросы к зачету
	Раздел 3. Средства защиты информации.	58	20	8		30	УК-2 ОПК-9 ПК-1	
12	Тема: Процесс развития средств и методов защиты информации. Этапы развития системы защиты информации в настоящее время. Комплексный подход к построению системы защиты информации. /лз/	2	2				УК-2 ОПК-9 ПК-1	Фронтальный опрос
13	Тема: Классические шифры перестановки/np/	2		2			УК-2 ОПК-9 ПК-1	Отчет по прак. работе
14	Тема: Системный подход к построению системы защиты информации. Цели задачи системы защиты информации. Этапы и порядок проведения работ по созданию системы защиты информации. /ср/	4		2		2	УК-2 ОПК-9 ПК-1	Вопросы к зачету
15	Тема: Структура систем защиты информации на современном этапе. Методы (виды) обеспечения защиты информации. /лз/	2	2				УК-2 ОПК-9 ПК-1	Тест по теме
16	Тема: Методы криптоанализа классических шифров. /np/	2		2			УК-2 ОПК-9 ПК-1	Отчет по прак. работе
17	Тема: Обеспечение режима конфиденциальности при работе с защищаемой информацией. /ср/	6		2		4	УК-2 ОПК-9 ПК-1	Реферат
18	Тема: Контроль за соблюдением требований информационной безопасности и защиты информации. /лз/	2	2				УК-2 ОПК-9 ПК-1	Фронтальный опрос
19	Тема: Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа. /np/	2		2			УК-2 ОПК-9 ПК-1	Доклад с презентацией
20	Тема: Ответственность за правонарушения информационной безопасности и защиты информации. /ср/	6		2		4	УК-2 ОПК-9 ПК-1	Вопросы к зачету
21	Тема: Административная	2		2			УК-2	Блиц опрос

	ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. /лз/						ОПК-9 ПК-1	
22	Тема: Уголовная ответственность за правонарушения в области защиты государственной тайны. /лз/	2		2			УК-2 ОПК-9 ПК-1	Устный опрос
23	Тема: Уголовная ответственность за правонарушения в области конфиденциальной информации. /ср/	2				2	УК-2 ОПК-9 ПК-1	Реферат
	контроль	36						
	Всего	108	14	30		28		

Для заочной 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. Понятие и сущность информационной безопасности и защиты информации.	30	2	2			26		
1	Тема: Необходимость и значимость нормативно-правового определения основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. /лз/	2	2				УК-2 ОПК-9 ПК-1	Устный опрос	
2	Защита документов MS Office /пр/	2		2			УК-2 ОПК-9 ПК-1	Отчет по практ.работе	
3	Тема: Основные компоненты безопасности государства и доминирующая роль ИБ. Становление и развитие понятия «информационная безопасность». Связь ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации. /ср/	8					УК-2 ОПК-9 ПК-1	Вопросы к зачету	
4	Тема: Основные угрозы информационной безопасности. Классификация угроз	4					УК-2 ОПК-9 ПК-1	Блиц-опрос	

	безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. /ср/							
5	Тема: Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). /ср/	4				4	УК-2 ОПК-9 ПК-1	Доклад с презентацией
6	Тема: Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз. /ср/	10				10	УК-2 ОПК-9 ПК-1	Реферат
	Раздел 2. Основные уровни информационной безопасности.	18	2			16		
7	Тема: Правовой и административный уровень обеспечения информационной безопасности /лз/	2	-			2	УК-2 ОПК-9 ПК-1	Устный опрос
8	Тема: Базовые методы криптографического преобразования данных. /ср/	2				2	УК-2 ОПК-9 ПК-1	Отчет по прак.работе
9	Тема: Программно-технический уровень обеспечения защиты информации /ср/	4				4	УК-2 ОПК-9 ПК-1	Блиц опрос
10	Тема: Использование методов замены для шифрования данных. /ср/	2				2	УК-2 ОПК-9 ПК-1	Отчет по прак.работе
11	Тема: Процедурный уровень информационной безопасности /ср/	8				8	УК-2 ОПК-9 ПК-1	Вопросы к зачету
	Раздел 3. Средства защиты информации.	60	2	2		56	УК-2 ОПК-9 ПК-1	
12	Тема: Процесс развития средств и методов защиты информации. Этапы развития системы защиты информации в настоящее время Комплексный подход к построению системы защиты информации. /лз/	2	2				УК-2 ОПК-9 ПК-1	Фронтальный опрос
13	Тема: Классические	2		2			УК-2	Отчет по

	шифры перестановки/ <i>np</i> /					ОПК-9 ПК-1	прак.работе
14	Тема: Системный подход к построению системы защиты информации Цели задачи системы защиты информации. Этапы и порядок проведения работ по созданию системы защиты информации. / <i>ср</i> /	8			8	УК-2 ОПК-9 ПК-1	Вопросы к зачету
15	Тема: Структура систем защиты информации на современном этапе. Методы (виды) обеспечения защиты информации. / <i>ср</i> /	4			4	УК-2 ОПК-9 ПК-1	Тест по теме
16	Тема: Методы криптоанализа классических шифров. / <i>ср</i> /	2			2	УК-2 ОПК-9 ПК-1	Отчет по прак.работе
17	Тема: Обеспечение режима конфиденциальности при работе с защищаемой информацией. / <i>ср</i> /	8			8	УК-2 ОПК-9 ПК-1	Реферат
18	Тема: Контроль за соблюдением требований информационной безопасности и защиты информации. / <i>ср</i> /	4			4	УК-2 ОПК-9 ПК-1	Фронтальный опрос
19	Тема: Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа. / <i>ср</i> /	4			4	УК-2 ОПК-9 ПК-1	Доклад с презентацией
20	Тема: Ответственность за правонарушения информационной безопасности и защиты информации. / <i>ср</i> /	6			6	УК-2 ОПК-9 ПК-1	Вопросы к зачету
21	Тема: Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. / <i>ср</i> /	4			4	УК-2 ОПК-9 ПК-1	Блиц опрос
22	Тема: Уголовная ответственность за правонарушения в области защиты государственной тайны. / <i>ср</i> /	4			4	УК-2 ОПК-9 ПК-1	Устный опрос
23	Тема: Уголовная ответственность за правонарушения в области конфиденциальной информации. / <i>ср</i> /	4			4	УК-2 ОПК-9 ПК-1	Реферат
24	Контроль	8					
	Всего	108	2	6	92		

5.2. Тематика лабораторных занятий

Учебным планом не предусмотрены

5.3. Примерная тематика курсовых работ

Учебным планом не предусмотрены

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 текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Описание шкал оценивания степени сформированности компетенций

Компетенции	Зачтено			Не зачтено Ниже порогового уровня (неудовлетворительно) (до 55 % баллов)
	Высокий уровень (отлично) (86-100% баллов)	Средний уровень (хорошо) (71-85% баллов)	Низкий уровень (удовлетворительно) (56-70% баллов)	

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Определяет полное знание совокупности взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм	УК-2.1. Определяет знание совокупности взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм	УК-2.1. В целом определяет знание совокупности взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм	УК-1.2. Определяет фрагментарное знание совокупности взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм
	УК-2. Определяет ресурсное обеспечение для достижения поставленной цели	УК-2.2. Определяет ресурсное обеспечение для достижения поставленной цели.	УК-2.2. В целом умеет определять ресурсное обеспечение для достижения поставленной цели.	УК-2.2. Не умеет определять ресурсное обеспечение для достижения поставленной цели.
	УК-2.3. Определяет ожидаемые результаты решения поставленных задач	УК-2.3. Определяет основные ожидаемые результаты решения поставленных задач	УК-2.3 Определяет в целом ожидаемые результаты решения поставленных задач	УК-2.3. Не владеет навыками определения ожидаемые результаты решения поставленных задач
ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Умеет полностью использовать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Знает основные принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	В целом знает основные принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Не знает основные принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
	Умеет полностью использовать современные информационные технологий и принципы для решения задач профессиональной деятельности	Умеет использовать современные информационные технологий и принципы для решения задач профессиональной деятельности	В целом умеет использовать современные информационные технологий и принципы для решения задач профессиональной деятельности	Умеет использовать современные информационные технологий и принципы для решения задач профессиональной деятельности
	Владеет в полном объеме навыками применения современных информационных технологий при решении задач профессиональной деятельности.	Владеет навыками применения современных информационных технологий при решении задач профессиональной деятельности.	В целом владеет навыками применения современных информационных технологий при решении задач профессиональной деятельности.	Не владеет навыками применения современных информационных технологий при решении задач профессиональной деятельности.

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 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:

УК-2

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними.
2. Современные средства защиты информации.
3. Современные системы компьютерной безопасности.
4. Современные средства противодействия экономическому шпионажу.
5. Современные криптографические системы.

ОПК-9

6. Криптоанализ, современное состояние.
7. Правовые основы защиты информации.
8. Технические аспекты обеспечения защиты информации. Современное состояние.
9. Атаки на систему безопасности и современные методы защиты.
10. Современные пути решения проблемы информационной безопасности РФ.

Критерии оценки доклада, сообщения, реферата:

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

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

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

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

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

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

Отметка «неудовлетворительно» ставится, если:

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

7.2.2. Примерные вопросы к итоговой аттестации (зачет)

УК-2

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?

9. Какие виды сетевых атак имеются?
 10. Что включает борьба с атаками на уровне приложений?
 11. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
 12. В чем заключается распределенное хранение файлов?
 13. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
 14. Какие уровни информационной защиты существуют, их основные составляющие?
 15. В чем заключаются задачи криптографии?
 16. Зачем нужны ключи?
 17. Какая схема шифрования называется многоалфавитной подстановкой?
 18. Какие системы шифрования вы знаете?
 19. Что включает в себя защита информации от несанкционированного доступа?
 20. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
 21. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
 22. Какой процесс называется аутентификацией пользователя?
 23. Какие схемы аутентификации вы знаете?
 24. Какие требования предъявляются к современным криптографическим системам защиты информации?
- ОПК-9**
25. Какими способами можно проверить систему безопасности?
 26. Что является основными характеристиками технических средств защиты информации?
 27. Какие требования предъявляются к межсетевым экранам?
 28. Какие имеются показатели защищенности межсетевых экранов?
 29. Какие атаки системы снаружи вы знаете?
 30. Какая программа называется вирусом?
 31. Какая атака называется атакой отказа в обслуживании?
 32. Какие виды вирусов вы знаете?
 33. Как распространяются вирусы?
 34. Какие методы обнаружения вирусов вы знаете?
 35. Какие задачи решает система компьютерной безопасности?
 36. Какие пути защиты информации в локальной сети существуют?
 37. Какие задачи решают технические средства противодействия экономическому шпионажу?
 38. Какие международные документы регламентируют деятельность по обеспечению защиты информации?
 39. Что понимают под политикой информационной безопасности?
 40. Что включает в себя политика информационной безопасности РФ?
 41. Какие нормативные документы РФ определяют концепцию защиты информации?

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

8.1. Основная литература:

1. Бабаш, А. В. История защиты информации в зарубежных странах: учебное пособие / А. В. Бабаш, Д. А. Ларин. - Москва: РИОР: ИНФРА-М, 2020. - 284 с. - ISBN 978-5-369-01844-6. - URL: <https://znanium.com/catalog/product/1081362>
2. Башлы, П. Н. Информационная безопасность и защита информации : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222с. - ISBN 978-5-369-01178-2. - URL: <https://znanium.com/catalog/product/405000>
3. Баранова, Е. К. Основы информатики и защиты информации: учебное пособие / Е.К. Баранова Е.К. - М.: РИОР, ИНФРА-М, 2018. - 183 с. - ISBN 978-5-369-01169-0. - URL: <https://znanium.com/catalog/product/959916>
4. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Москва: РИОР: ИНФРА-М, 2020. - 336 с. - ISBN 978-5-369-01761-6. - URL: <https://znanium.com/catalog/product/1114032>

8.2. Дополнительная литература:

1. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - ISBN 978-5-369-01759-3. - URL: <https://znanium.com/catalog/product/1018901>

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

9. 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 14.05.2025г. до 14.05.2026г.
2025-2026 учебный год	Электронно-библиотечная система «Лань». Договор № 10 от 11.02.2025 г. Электронный адрес: https://e.lanbook.com	от 11.02.2025г. до 11.02.2026г.
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 оснащённости аудиторий можно ознакомиться на сайте университета, в разделе материально-технического обеспечения и оснащённости образовательного процесса по адресу: <https://kchgu.ru/sveden/objects/>

9.3. Необходимый комплект лицензионного программного обеспечения

- Microsoft Windows (Лицензия № 60290784), бессрочная
- Microsoft Office (Лицензия № 60127446), бессрочная
- ABBY FineReader (лицензия № FCRP-1100-1002-3937), бессрочная
- CalculateLinux (внесён в ЕРПП 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 28.02.2025г. Срок действия лицензии с 27.02.2025г. по 07.03.2027г.

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 Elsevier <http://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](http://kchgu.ru)», 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
Переутверждена ОПВО. Обновлены: учебный план, календарный учебный график, РПД, РПП, программы ГИА, воспитания, календарный план воспитательной работы. Обновлены договоры: 1. На антивирус Касперского. (Договор №56/2023 от 25 января 2023г.). Действует до 03.03.2025г. 2. На антивирус Касперского. (Договор № 0379400000325000001/1 от 28.02.2025г. Действует по 07.03.2027г. 3. Договор № 10 от 11.02.2025г. эбс «Лань». Действует по 11.02.2026г. 4. Договор № 238 эбс ООО «Знаниум» от 23.04.2024г. Действует до 11 мая 2025г. Договор № 249-эбс ООО «Знаниум» от 14.05.2025г. Действует до 14.05.2026г.	29.04.2025г., протокол № 8	30.04.2025г., протокол № 8