

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

Педагогический факультет

**Кафедра теории и методики преподавания гуманитарных
и естественно-научных дисциплин**

УТВЕРЖДАЮ
И.о.проректора
М.Х. Чанкаев
29. 04. 2026 г., протокол № 7

Рабочая программа дисциплины

**Проектирование безопасной
цифровой образовательной среды**

(наименование дисциплины (модуля))

Направление подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки)

(шифр, название направления)

Направленность (профиль) подготовки
"Начальное образование; дошкольное образование"

Квалификация выпускника
бакалавр

Форма обучения
Очная/заочная

Год начала подготовки - 2023

Карачаевск, 2026

Составитель: ст.пр. Джанибекова Ф.О.

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) утвержденного приказом Министерства образования и науки Российской Федерации от 22.02.2018 № 125, образовательной программой высшего образования по направлению подготовки 44.03.05 – Педагогическое образование (с двумя профилями подготовки), профиль – Начальное образование; дошкольное образование; ОП; локальными актами КЧГУ.

Рабочая программа рассмотрена и утверждена на заседании кафедры теории и методики преподавания гуманитарных и естественно-научных дисциплин на 2026-2027 учебный год, протокол № 7 от 23.03.2026 г.

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.....	5
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.....	7
5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....	8
5.1. Разделы дисциплины и трудоемкость по видам учебных занятий.....	8
(в академических часах)	8
5.2. Тематика лабораторных занятий	10
5.3. Примерная тематика курсовых работ.....	10
6. Образовательные технологии	10
7. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю).....	11
7.1. Описание шкал оценивания степени сформированности компетенций.....	11
7.2. Типовые контрольные задания или иные учебно-методические материалы, необходимые для оценивания степени сформированности компетенций в процессе освоения учебной дисциплины	19
7.2.1. Типовые темы к письменным работам, докладам и выступлениям:	19
7.2.2. Примерные вопросы к итоговой аттестации (зачет).....	20
7.2.3. Тестовые задания для проверки знаний студентов	21
7.2.4. Бально-рейтинговая система оценки знаний бакалавров.....	25
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины. Информационное обеспечение образовательного процесса.....	26
8.1. Основная литература:	26
8.2. Дополнительная литература:.....	26
9. Методические указания для обучающихся по освоению учебной дисциплины (модуля)	27
10. Требования к условиям реализации рабочей программы дисциплины (модуля)	27
10.1. Общесистемные требования	27
10.2. Материально-техническое и учебно-методическое обеспечение дисциплины	28
10.3. Необходимый комплект лицензионного программного обеспечения	28
10.4. Современные профессиональные базы данных и информационные справочные системы..	29
11. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья.....	29
12. Лист регистрации изменений.....	30

1. Наименование дисциплины(модуля)

Проектирование безопасной цифровой образовательной среды

Целью освоения дисциплины является формирование у будущих педагогов профессиональных компетенций в области проектирования, организации и поддержки безопасной цифровой образовательной среды в школе, обеспечивающей защиту персональных данных, фильтрацию опасного контента и психологическое благополучие учащихся.

Для достижения цели ставятся задачи:

1. Знаниевые (теоретические) задачи:

- Изучить нормативно-правовую базу: Сформировать четкое понимание законов РФ (ФЗ «Об образовании в РФ», ФЗ «О персональных данных») и требований СанПиН, регулирующих цифровую среду школы.
- Освоить классификацию рисков: Научить будущих учителей распознавать технические (фишинг, вирусы), контентные и социально-психологические (кибербуллинг, деструктивные сообщества) угрозы в сети.
- Изучить архитектуру безопасной ЦОС: Ознакомить студентов с принципами работы верифицированных отечественных платформ (ФГИС «Моя школа», «Сферум») и ролевыми моделями доступа к данным.

2. Деятельностные (практические) задачи:

- Научить проектированию среды: Развить навыки разработки локальных актов, регламентов использования гаджетов и комплексных моделей безопасной ЦОС для конкретного класса или школы.
- Сформировать навыки реагирования: Отработать алгоритмы действий педагога при выявлении фактов кибератак, утечки данных или психологического насилия (травли) в школьных чатах и соцсетях.
- Обучить методам фильтрации и защиты: Сформировать базовые умения по оценке эффективности контент-фильтров и защите персональных данных учащихся.

3. Методические и просветительские задачи:

- Развить методические навыки: Научить студентов проектировать и проводить уроки, классные часы и внеурочные мероприятия по цифровой гигиене для школьников разного возраста.
- Подготовить к работе с родителями: Сформировать умение организовывать родительские собрания и консультации по вопросам медиабезопасности и домашнего родительского контроля.

Цели и задачи дисциплины определены в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) Направленность (профиль) подготовки "Начальное образование; дошкольное образование "(квалификация – «бакалавр»).

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Проектирование безопасной цифровой образовательной среды» (Б1.В.ДВ.05.02) относится к дисциплинам по выбору части, формируемой участниками образовательных отношений.

Дисциплина (модуль) изучается на 5 курсе в А(10) семестре.

Индекс	Б1.В.ДВ.05.02
Требования к предварительной подготовке обучающегося:	
Учебная дисциплина «Проектирование безопасной цифровой образовательной среды» является дисциплиной по выбору, опирается на входные знания, полученные в ходе обучения курсу школьной информатики и дисциплине «Системы искусственного интеллекта».	
Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Изучение дисциплины «Проектирование безопасной цифровой образовательной среды» основой для изучения дисциплин учебного плана, содержание которых связано с углублением профессиональных знаний в указанной предметной области, выполнения курсовой и выпускной квалификационной работ	

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

Процесс изучения дисциплины направлен на формирование следующих компетенций обучающегося:

Код компетенций	Содержание компетенции в соответствии с ФГОС ВО/ ОП ВО	Индикаторы достижения компетенций	Декомпозиция компетенций (результаты обучения) в соответствии с установленными индикаторами
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 задач. УК-2.3. Использует инструменты и техники цифрового моделирования для реализации образовательных процессов	Знать: Ресурсные возможности современной школы (сервисы ФГИС «Моя школа», платформу «Сферум», техническое оснащение классов) для построения безопасной ЦОС. Правовые ограничения и требования (ФЗ-152, ФЗ-273, СанПиН), регламентирующие распределение ресурсов и постановку задач при внедрении ИКТ. Потенциальные риски (утечка данных, контентные угрозы, деструктивное поведение в чатах) и ограничения (недостаточная цифровая грамотность участников, технические сбои) при реализации ЦОС. Критерии оценки эффективности защищенной цифровой среды и планируемые результаты ее внедрения. Принципы, методы и программные инструменты цифрового моделирования безопасной ИОС (информационно-образовательной среды). Архитектуру и функционал ролевых моделей доступа в отечественных экосистемах (администратор, учитель, ученик, родитель) Уметь: Декомпозировать общую цель проектирования безопасной ЦОС на систему конкретных управленческих и педагогических задач. Оценивать материально-

			технические, временные и кадровые ресурсы образовательной организации для развертывания верифицированного ПО. Прогнозировать появление киберугроз и психологических рисков (кибербуллинг) в цифровом пространстве класса/школы. Сопоставлять затраченные ресурсы с планируемыми показателями защищенности и качества образовательного процесса. Проектировать виртуальные пространства уроков, сетевых сообществ и классных часов с заданными параметрами безопасности. Моделировать безопасные сценарии взаимодействия участников образовательного процесса с использованием верифицированных инструментов совместной работы Владеть: Алгоритмами планирования комплекса мероприятий по защите информации и организации безопасного онлайн-обучения в рамках правового поля школы Методами риск-менеджмента в области информационной безопасности образовательной организации. Технологией разработки локальных регламентов (например, правил использования личных гаджетов) для предотвращения инцидентов. Практическими навыками конструирования безопасной модели ЦОС под конкретные дидактические задачи с применением отечественных платформенных решений
ПК-1	Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач	ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета). ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО. ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять	Знать: Нормативно-правовую базу, регулирующую безопасность ЦОС в РФ (ФЗ-273, ФЗ-152, СанПиН, требования к ограничению вредоносной информации). Классификацию и специфику угроз в цифровой среде (технические, контентные, коммуникативные, психологические). Дидактические возможности и архитектуру верифицированных отечественных платформ (ФГИС «Моя школа», ИКОС «Сферум»).

		методы, приемы и технологии обучения, в том числе ин формационные.	Требования ФГОС общего образования к формированию безопасной информационно-образовательной среды. Методику проведения учебных занятий и классных часов по цифровой гигиене и медиабезопасности для школьников. Специфику применения безопасных ИКТ-технологий, инструментов совместной работы и облачных сервисов в обучении. Уметь: Определять и структурировать ключевые элементы безопасной цифровой среды в рамках своей предметной области. Классифицировать цифровые образовательные ресурсы по уровню их безопасности и методической ценности. Проводить экспертизу электронных учебных материалов на предмет отсутствия скрытых угроз, агрессивной рекламы и деструктивного контента. Адаптировать учебное содержание для различных форм обучения (очное, дистанционное, смешанное), соблюдая гигиенические нормы работы с техникой (СанПиН). Разрабатывать технологические карты уроков и сценарии внеклассных мероприятий с использованием безопасного инструментария ЦОС. Владеть: Понятийным и терминологическим аппаратом в области информационной безопасности и проектирования ЦОС. Навыками фильтрации и верификации цифровых источников информации для конструирования безопасного учебного процесса. Методическими приемами формирования у школьников навыков безопасного поведения в сети Интернет
--	--	--	--

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 2 ЗЕТ, 72 академических часа.

Объём дисциплины	Всего часов	Всего часов
------------------	-------------	-------------

	для очной формы обучения	для заочной формы обучения
Общая трудоемкость дисциплины	72	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)		
Аудиторная работа (всего):	36	6
в том числе:		
лекции	12	2
семинары, практические занятия	22	4
практикумы	Не предусмотрено	
лабораторные работы	Не предусмотрено	
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)	38	62
Контроль самостоятельной работы		4
Вид промежуточной аттестации обучающегося (зачет / экзамен)	зачет	зачет

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

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

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			
1.	Раздел 1. Нормативно-правовое регулирование и архитектура безопасной ЦОС							
	Тема 1.1. Нормативная база и понятия ЦОС в РФ.	8	2	2		4	ПК-1	Устный опрос Задания к практической работе Тест
	Тема 1.2. Архитектура и гигиенические требования к ЦОС.	12	2	4		6	ПК-1	Устный опрос Задания к практической работе Тест
2.	Раздел 2. Киберугрозы, контентная и психологическая безопасность в школе							
	Тема 2.1. Технические и контентные риски в образовании.	12	2	4		6	ПК-1	Устный опрос Задания к практической работе Тест
	Тема 2.2. Психологические	14	2	4		8	ПК-1	Устный опрос

	угрозы: кибербуллинг и деструктивный контент.							Задания к практической работе Тест
3.	Раздел 3. Технологии проектирования и методики защиты цифровой среды							
	Тема 3.1. Выбор безопасных платформ (Сферум, ФГИС «Моя школа») и защита данных.	12	2	4		6	ПК-1	Устный опрос Задания к практической работе Тест
	Тема 3.2. Методика обучения школьников цифровой гигиене.	14	2	4		8	ПК-1	Устный опрос Задания к практической работе Тест
	Всего	72	12	22		38		

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
				Лек	Пр	Лаб		
1.	Раздел 1. Нормативно-правовое регулирование и архитектура безопасной ЦОС							
	Тема 1.1. Нормативная база и понятия ЦОС в РФ.	8	2				6	ПК-1 Устный опрос Задания к практической работе Тест
	Тема 1.2. Архитектура и гигиенические требования к ЦОС.	12					12	ПК-1 Устный опрос Задания к практической работе Тест
2.	Раздел 2. Киберугрозы, контентная и психологическая безопасность в школе							
	Тема 2.1. Технические и контентные риски в образовании.	12		2			10	ПК-1 Устный опрос Задания к практической работе Тест
	Тема 2.2. Психологические угрозы: кибербуллинг и деструктивный контент.	14					14	ПК-1 Устный опрос Задания к практической работе Тест
3.	Раздел 3. Технологии проектирования и методики защиты цифровой среды							
	Тема 3.1. Выбор безопасных платформ (Сферум, ФГИС «Моя школа») и защита данных.	12		2			10	ПК-1 Устный опрос Задания к практической работе Тест
	Тема 3.2. Методика обучения школьников цифровой гигиене.	14					14	ПК-1 Устный опрос Задания к практической работе Тест

	Контроль	4						
	Всего	72	2	4		62		

5.2. Тематика лабораторных занятий

Учебным планом не предусмотрены

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.

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.

Лекция – одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала. Она предшествует всем другим формам организации учебного процесса, позволяет оперативно актуализировать учебный материал дисциплины. Для повышения эффективности лекций целесообразно воспользоваться следующими рекомендациями:

- четко и ясно структурировать занятие;
- рационально дозировать материал в каждом из разделов;
- использовать простой, доступный язык, образную речь с примерами и сравнениями;
- отказаться, насколько это возможно, от иностранных слов;
- использовать наглядные пособия, схемы, таблицы, модели, графики и т. п.;
- применять риторические и уточняющие понимание материала вопросы;
- обращаться к техническим средствам обучения.

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

Практические занятия проводятся в форме групповой дискуссии, «мозговой атаки», решения практических задач и др.

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

1. Обсуждение в группах

Групповое обсуждение какого-либо вопроса направлено на нахождение 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
УК-2					
Базовый	Знать: Ресурсные возможности современной школы (сервисы ФГИС «Моя школа», платформу «Сферум», техническое оснащение классов) для построения безопасной	Студент имеет грубые ошибки в базовых понятиях. Не знает ресурсных возможностей образовательных платформ и требований законодательства	Знания поверхностные. Студент знает основные законы, но затрудняется перечислить ограничения, которые они накладывают на учебный процесс	Студент твердо знает теоретический материал, правовые нормы и ограничения. Хорошо понимает классификацию рисков (утечки данных, кибер-	

	ЦОС. Правовые ограничения и требования (ФЗ-152, ФЗ-273, Сан-ПиН), регламентирующие распределение ресурсов и постановку задач при внедрении ИКТ. Потенциальные риски (утечка данных, контентные угрозы, деструктивное поведение в чатах) и ограничения (недостаточная цифровая грамотность участников, технические сбои) при реализации ЦОС. Критерии оценки эффективности защищенной цифровой среды и планируемые результаты ее внедрения. Принципы, методы и программные инструменты цифрового моделирования безопасной ИОС (информационно-образовательной среды). Архитектуру и функционал ролевых моделей доступа в общественных экосистемах (администратор, учитель, ученик, родитель)	тельства. Не способен сформулировать риски и ограничения при проектировании ЦОС	цесс. Путает критерии оценки рисков, слабо ориентируется в принципах цифрового моделирования.	буллинг). При описании архитектуры ролевых моделей доступа в ЦОС допускает 1–2 несущественные неточности.	
	Уметь: Декомпозировать общую цель проектирования безопасной ЦОС на систему конкретных управленческих и педагогических задач. Оценивать материально-технические, временные и кадровые ресурсы образовательной организации для развертывания верифицированного ПО. Прогнозировать появление киберугроз и психологических рисков (кибербуллинг) в цифровом пространстве класса/школы.	Студент не умеет распределять задачи и оценивать ресурсы для достижения цели. Полностью отсутствует навык прогнозирования рисков. Не способен спроектировать или запустить простейшую модель безопасного цифрового взаимодействия.	Умения носят репродуктивный характер. Студент может распределить задачи и ресурсы только по готовому шаблону. Затрудняется самостоятельно спрогнозировать риски кибербуллинга или смоделировать безопасный сценарий онлайн-взаимодействия без помощи преподавателя	Студент успешно справляется с постановкой задач и оценкой рисков в ЦОС. Умеет проектировать сетевые сообщества и учебные сессии на базе отечественного ПО. При расчете ресурсного обеспечения или моделировании ролей доступа допускает мелкие оплошности.	

	Сопоставлять затраченные ресурсы с планируемыми показателями защищенности и качества образовательного процесса. Проектировать виртуальные пространства уроков, сетевых сообществ и классных часов с заданными параметрами безопасности. Моделировать безопасные сценарии взаимодействия участников образовательного процесса с использованием верифицированных инструментов совместной работы				
	Владеть: Алгоритмами планирования комплекса мероприятий по защите информации и организации безопасного онлайн-обучения в рамках правового поля школы Методами риск-менеджмента в области информационной безопасности образовательной организации. Технологией разработки локальных регламентов (например, правил использования личных гаджетов) для предотвращения инцидентов. Практическими навыками конструирования безопасной модели ЦОС под конкретные дидактические задачи с применением отечественных платформенных решений	Студент не владеет навыками риск-менеджмента в цифровой среде. Практические навыки разработки локальных регламентов, планирования мероприятий по защите информации и цифрового моделирования образовательных процессов полностью отсутствуют	Владение навыками неустойчиво. Методы управления рисками применяются хаотично. Навыки настройки ролевых моделей доступа и конструирования безопасной среды развиты слабо, студент делает серьезные ошибки при попытке адаптировать модель под конкретный класс.	Студент уверенно владеет технологией разработки внутренних инструкций (например, правил использования гаджетов) и техниками цифрового моделирования среды. Действует успешно, но в сложных нестандартных ситуациях управления рисками нуждается в самопроверке	
Повышенный	Знать: Ресурсные возможности современной школы (сервисы ФГИС «Моя школа», платформу «Сферум», техническое оснащение классов) для построения безопасной				Студент демонстрирует системные знания ресурсных возможностей школы и верифицированных платформ («Моя школа», «Сферум»). Четко

	ЦОС. Правовые ограничения и требования (ФЗ-152, ФЗ-273, СанПиН), регламентирующие распределение ресурсов и постановку задач при внедрении ИКТ. Потенциальные риски (утечка данных, контентные угрозы, деструктивное поведение в чатах) и ограничения (недостаточная цифровая грамотность участников, технические сбои) при реализации ЦОС. Критерии оценки эффективности защищенной цифровой среды и планируемые результаты ее внедрения. Принципы, методы и программные инструменты цифрового моделирования безопасной ИОС (информационно-образовательной среды). Архитектуру и функционал ролевых моделей доступа в общественных экосистемах (администратор, учитель, ученик, родитель)				знает все правовые ограничения (ФЗ-152, ФЗ-273, СанПиН), потенциальные киберриски и принципы цифрового моделирования образовательной среды
	Уметь: Декомпозировать общую цель проектирования безопасной ЦОС на систему конкретных управленческих и педагогических задач. Оценивать материально-технические, временные и кадровые ресурсы образовательной организации для развертывания верифицированного ПО. Прогнозировать появление киберугроз и психологических рисков (кибербуллинг) в цифровом пространстве класса/школы.				Студент безошибочно декомпозирует цель проектирования ЦОС на комплекс взаимосвязанных задач. Точно оценивает ресурсы, прогнозирует любые риски и умеет самостоятельно моделировать безопасные виртуальные пространства уроков с заданными параметрами защиты.

	Сопоставлять затраченные ресурсы с планируемыми показателями защищенности и качества образовательного процесса. Проектировать виртуальные пространства уроков, сетевых сообществ и классных часов с заданными параметрами безопасности. Моделировать безопасные сценарии взаимодействия участников образовательного процесса с использованием верифицированных инструментов совместной работы				
	Владеть: Алгоритмами планирования комплекса мероприятий по защите информации и организации безопасного онлайн-обучения в рамках правового поля школы Методами риск-менеджмента в области информационной безопасности образовательной организации. Технологией разработки локальных регламентов (например, правил использования личных гаджетов) для предотвращения инцидентов. Практическими навыками конструирования безопасной модели ЦОС под конкретные дидактические задачи с применением отечественных платформенных решений				Студент в совершенстве владеет алгоритмами планирования ИБ-мероприятий и методами риск-менеджмента в школе. Демонстрирует автоматизированные навыки разработки локальных регламентов и конструирования безопасных моделей ЦОС под любые дидактические задачи.
ПК-1					
Базовый	Знать: Нормативно-правовую базу, регулиющую безопасность ЦОС в РФ (ФЗ-273, ФЗ-152, СанПиН, требования к ограничению вредоносной	Студент демонстрирует полное отсутствие знаний или имеет грубые ошибки в базовых понятиях. Не знает требований ФЗ «О персональных	Знания носят фрагментарный или поверхностный характер. Студент знает основные законы и платформы, но затрудняется	Студент твердо знает теоретический материал и нормативно-правовую базу, ориентируется в классификации рисков. Допускает	

информации). Классификацию и специфику угроз в цифровой среде (технические, контентные, коммуникативные, психологические). Дидактические возможности и архитектуру верифицированных отечественных платформ (ФГИС «Моя школа», ИКОС «Сферум»). Требования ФГОС общего образования к формированию безопасной информационно-образовательной среды. Методику проведения учебных занятий и классных часов по цифровой гигиене и медиабезопасности для школьников. Специфику применения безопасных ИКТ-технологий, инструментов совместной работы и облачных сервисов в обучении.	данных» и СанПиН. Не ориентируется в структуре цифровой образовательной среды.	классифицировать угрозы. Не может подробно описать санитарно-гигиенические нормы (СанПиН) или структуру безопасной ЦОС без наводящих вопросов.	1–2 несущественные неточности или путаницу в формулировках при ответе на сложные вопросы по архитектуре ЦОС	
Уметь: Определять и структурировать ключевые элементы безопасной цифровой среды в рамках своей предметной области. Классифицировать цифровые образовательные ресурсы по уровню их безопасности и методической ценности. Проводить экспертизу электронных учебных материалов на предмет отсутствия скрытых угроз, агрессивной рекламы и деструктивного контента. Адаптировать учебное содержание для различных форм обучения (очное, дистанционное, смешанное), соблюдая гигиенические нормы работы с техникой (СанПиН).	Студент не умеет применять теоретические знания на практике. Не способен отличить безопасный верифицированный цифровой ресурс от опасного. Не может адаптировать материал для учебного занятия в ЦОС	Умения сформированы на минимальном уровне. Студент может отобрать цифровые ресурсы только по шаблону или готовому алгоритму. Затрудняется самостоятельно провести экспертизу контента на скрытые риски без помощи преподавателя	Студент успешно справляется с отбором и адаптацией цифрового контента, умеет классифицировать ресурсы по уровню безопасности. При решении практических задач или проектировании чек-листов допускает мелкие оплошности, которые может самостоятельно исправить	

	Разрабатывать технологические карты уроков и сценарии внеклассных мероприятий с использованием безопасного инструментария ЦОС				
	Владеть: Понятийным и терминологическим аппаратом в области информационной безопасности и проектирования ЦОС. Навыками фильтрации и верификации цифровых источников информации для конструирования безопасного учебного процесса. Методическими приемами формирования у школьников навыков безопасного поведения в сети Интернет	Студент не владеет профессиональной терминологией предметной области. Практические навыки настройки безопасной среды, защиты персональных данных и методические приемы работы со школьниками полностью отсутствуют	Владение навыками носит неустойчивый характер. Терминологический аппарат используется с трудом. Практические навыки защиты данных (настройка доступа, фильтрация) применяются не уверенно, студент допускает серьезные ошибки в методике ведения уроков по цифровой гигиене.	Студент уверенно владеет основными технологиями защиты данных и методиками обучения школьников кибербезопасности. При демонстрации практических навыков настройки платформ или моделирования уроков действует успешно, но иногда нуждается в самопроверке.	
Повышенный	Знать: Нормативно-правовую базу, регулиующую безопасность ЦОС в РФ (ФЗ-273, ФЗ-152, СанПиН, требования к ограничению вредоносной информации). Классификацию и специфику угроз в цифровой среде (технические, контентные, коммуникативные, психологические). Дидактические возможности и архитектуру верифицированных отечественных платформ (ФГИС «Моя школа», ИКОС «Сферум»). Требования ФГОС общего образования к формированию безопасной информационно-образовательной среды. Методику проведения учебных занятий и классных часов по цифровой гигиене и медиабезопасности для школьников.				В полном объеме демонстрирует глубокие, системные знания нормативной базы (ФЗ-273, ФЗ-152, СанПиН), безошибочно классифицирует все виды угроз в ЦОС. Свободно ориентируется в дидактических единицах предмета и архитектуре верифицированных отечественных платформ («Сферум», ФГИС «Моя школа»)

Специфику применения безопасных ИКТ-технологий, инструментов совместной работы и облачных сервисов в обучении.				
Уметь: Определять и структурировать ключевые элементы безопасной цифровой среды в рамках своей предметной области. Классифицировать цифровые образовательные ресурсы по уровню их безопасности и методической ценности. Проводить экспертизу электронных учебных материалов на предмет отсутствия скрытых угроз, агрессивной рекламы и деструктивного контента. Адаптировать учебное содержание для различных форм обучения (очное, дистанционное, смешанное), соблюдая гигиенические нормы работы с техникой (СанПиН). Разрабатывать технологические карты уроков и сценарии внеклассных мероприятий с использованием безопасного инструментария ЦОС				Студент самостоятельно, быстро и без ошибок проводит экспертизу цифрового контента. Безупречно структурирует элементы безопасной среды под конкретный класс, легко адаптирует учебные материалы под любые формы обучения (очное, ДОТ) в строгом соответствии с ФГОС и СанПиН.
Владеть: Понятийным и терминологическим аппаратом в области информационной безопасности и проектирования ЦОС. Навыками фильтрации и верификации цифровых источников информации для конструирования безопасного учебного процесса. Методическими приемами формирования у школьников навыков безопасного поведения в сети Интернет				Студент в совершенстве владеет понятийным аппаратом ИБ. Демонстрирует автоматизированные навыки безопасной настройки ЦОС (двухфакторная проверка, роли доступа). Владеет широким арсеналом методических приемов формирования цифровой гигиены у школьников.

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. **Правовое регулирование ИБ:** Эволюция законодательства РФ в сфере защиты персональных данных участников образовательного процесса (анализ правоприменительной практики ФЗ-152 в школе).
2. **Локальные акты школы:** Разработка пакета нормативных документов образовательной организации по обеспечению информационной безопасности.
3. **Гигиена и здоровье:** Проблема соблюдения требований актуальных СанПиН при проектировании гибридной и дистанционной моделей обучения.
4. **Архитектура ЦОС:** Сравнительный анализ архитектуры и дидактического потенциала верифицированных отечественных платформ (ФГИС «Моя школа» и ИКОС «Сферум»).
5. **Зарубежный опыт:** Международные стандарты и подходы к проектированию безопасной информационной среды в образовании: опыт и ограничения для РФ.
6. **Социальная инженерия:** Методы социальной инженерии и фишинга, ориентированные на педагогический состав, и способы защиты от них.
7. **Контентная фильтрация:** Белые и черные списки: принципы настройки и оценка эффективности систем контентной фильтрации в учебных заведениях.
8. **Кибербуллинг:** Педагогические технологии профилактики и раннего выявления кибербуллинга в подростковой среде.
9. **Алгоритм действий педагога:** Действия классного руководителя при обнаружении фактов вовлечения учащихся в деструктивные интернет-сообщества.
10. **Цифровая зависимость:** Интернет-аддикция и гейминг у школьников: психологические риски и методы педагогической коррекции.
11. **Школьные медиа:** Безопасность официального сайта и верифицированных аккаунтов школы в социальных сетях: риски компрометации контента.
12. **Ролевые модели доступа:** Проектирование матрицы прав доступа (администратор-педагог-ученик-родитель) в современной школьной LMS.
13. **Мобильные устройства:** Политика BYOD (Bring Your Own Device) в школе: за и против (разработка регламента использования личных гаджетов на уроках).
14. **Методика обучения:** Проектирование интерактивных форм обучения (квесты, квизы) цифровой гигиене для учащихся начальной / основной школы.
15. **Работа с семьей:** Методы эффективного взаимодействия педагога с родителями по вопросам обеспечения медиабезопасности детей в домашних условиях.
16. **Облачные технологии:** Риски и преимущества использования отечественных облачных сервисов для организации совместной проектной деятельности учащихся.

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)

Блок 1. Нормативно-правовое регулирование и архитектура безопасной ЦОС

1. Понятие «цифровая образовательная среда» (ЦОС) и критерии ее безопасности в контексте требований ФГОС общего образования.

2. Федеральный закон «О персональных данных» (ФЗ-152): обязанности образовательной организации и педагога при обработке персональных данных учащихся.

3. Законодательное регулирование защиты детей от информации, причиняющей вред их здоровью и развитию (ФЗ-436): классификация вредоносного контента.

4. Актуальные санитарные правила и нормы (СанПиН): гигиенические требования к использованию электронных средств обучения (ЭСО) на уроках в разных классах.

5. Локальные нормативные акты школы по обеспечению информационной безопасности: структура, назначение и порядок разработки.

6. Архитектура, функциональные возможности и дидактический потенциал ФГИС «Моя школа» как безопасной образовательной платформы.

7. Информационно-коммуникационная образовательная среда (ИКОС) «Сферум»: инструменты безопасного взаимодействия участников образовательного процесса.

Блок 2. Риски, киберугрозы и психологическая безопасность в школе

8. Классификация рисков в ЦОС: технические, контентные, коммуникативные и потребительские угрозы в образовании.

9. Социальная инженерия и фишинг в сфере образования: методы манипуляции, признаки атак на педагогов и способы защиты от них.

10. Системы контентной фильтрации (СКФ) в образовательных организациях: принципы работы, белые и черные списки, оценка эффективности.

11. Феномен кибербуллинга в подростковой среде: виды, психологические последствия и маркеры выявления травли в школьных цифровых сообществах.

12. Алгоритм действий классного руководителя и администрации школы при выявлении факта кибербуллинга или интернет-травли среди учащихся.

13. Сетевой груминг и вовлечение несовершеннолетних в деструктивные интернет-сообщества: признаки опасного поведения ребенка в сети.

14. Интернет-зависимость, гейминг и синдром упущенной выгоды (FoMO): педагогические методы профилактики цифровой аддикции у школьников.

Блок 3. Проектирование, моделирование и методики защиты цифровой среды

15. Принципы проектирования безопасной модели ЦОС для конкретной образовательной организации (ресурсы, ограничения, правовое поле).

16. Управление рисками (риск-менеджмент) при интеграции новых цифровых сервисов и инструментов в учебный процесс школы.

17. Ролевые модели доступа (матрица прав администратора, учителя, ученика, родителя) как инструмент защиты данных в школьных информационных системах.

18. Политика BYOD (Bring Your Own Device) в современной школе: правовые рамки, технические риски и правила разработки регламента использования личных гаджетов.
19. Методика отбора верифицированного цифрового контента для уроков в соответствии с дидактическими единицами предмета.
20. Технология проектирования уроков и внеклассных мероприятий (квесты, квизы, интерактивные беседы) по цифровой гигиене для школьников.
21. Организация просветительской работы с родителями по вопросам настройки домашнего родительского контроля и обеспечения медиабезопасности детей.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если вопросы раскрыты, изложены логично, без существенных ошибок, показано умение иллюстрировать теоретические положения конкретными примерами, продемонстрировано усвоение ранее изученных вопросов, сформированность компетенций, устойчивость используемых умений и навыков. Допускаются незначительные ошибки;
- оценка «не зачтено» выставляется, если не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, которые не исправлены после нескольких наводящих вопросов; не сформированы компетенции, умения и навыки.

**Критерии оценки устного ответа на вопросы по дисциплине
«Компьютерная графика»:**

- ✓ 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

Раздел 1. Нормативно-правовое регулирование и архитектура безопасной ЦОС

1. Какой федеральный закон в РФ регулирует отношения, связанные с обработкой личных данных учащихся и педагогов?

- А) ФЗ-273 «Об образовании в РФ»
- Б) ФЗ-152 «О персональных данных»
- В) ФЗ-436 «О защите детей от информации...»

• Г) ФЗ-149 «Об информации, информационных технологиях и о защите информации»

2. Каким нормативным документом в РФ установлены гигиенические нормативы и требования к использованию электронных средств обучения (ЭСО) в школах?

- А) ФГОС общего образования
- Б) Профессиональный стандарт педагога
- В) Санитарные правила и нормы (СанПиН)
- Г) Устав образовательной организации

3. Согласно санитарным правилам, использование мобильных телефонов (смартфонов) для образовательных целей на уроке:

• А) Разрешено без ограничений во всех классах
• Б) Разрешено только в старших (10–11) классах
• В) Не допускается (запрещено использовать вместо персонального компьютера или планшета)

- Г) Допускается только при наличии письменного согласия родителей

4. Какая информационная система является официальной федеральной платформой, содержащей верифицированный цифровой образовательный контент в РФ?

- А) Moodle
- Б) ФГИС «Моя школа»
- В) Google Workspace for Education
- Г) Coursera

5. Для безопасного онлайн-взаимодействия и ведения школьных чатов Минпросвещения РФ рекомендует использовать:

- А) Telegram
- Б) WhatsApp
- В) ИКОС «Сферум» (ВК Мессенджер)
- Г) Viber

6. Что такое «ролевая модель доступа» при проектировании безопасной ЦОС школы?

• А) Распределение учебных ролей во время деловой игры на уроке
• Б) Разграничение прав пользователей (администратор, учитель, ученик, родитель) на просмотр и редактирование данных в системе

- В) Психологическая модель поведения учителя в условиях цифровизации
- Г) Ограничение времени нахождения ученика за компьютером

7. Какое из перечисленных действий педагога является грубым нарушением ФЗ «О персональных данных»?

• А) Публикация списка оценок учащихся с указанием их полных ФИО в открытом личном блоге или публичной группе соцсети

- Б) Заполнение электронного журнала во ФГИС «Моя школа»
- В) Передача списка класса завучу школы по внутренним защищенным каналам связи

- Г) Отправка индивидуального сообщения родителю о согласовании даты экскурсии

Раздел 2. Киберугрозы, контентная и психологическая безопасность в школе

8. Вид мошенничества, целью которого является получение доступа к конфиденциальным данным (паролям, логинам) сотрудников школы через поддельные письма или сообщения от имени администрации, называется:

- А) Фишинг
- Б) Спам
- В) DDoS-атака
- Г) Буткит

9. Как называется преднамеренное, систематическое и агрессивное преследование, издевательство или травля человека с использованием цифровых технологий (соцсетей, мессенджеров)?

- А) Стриминг
- Б) Кибербуллинг
- В) Груминг
- Г) Флуд

10. Установление взрослым человеком доверительных отношений с несовершеннолетним в сети Интернет с целью последующей сексуальной эксплуатации или шантажа — это:

- А) Краудсорсинг
- Б) Кибербуллинг
- В) Сетевой груминг
- Г) Фишинг

11. Какое техническое или программное средство обязана применять школа для блокировки доступа учащихся к экстремистским материалам и нецензурному контенту?

- А) Антивирус Касперского
- Б) Систему контентной фильтрации (СКФ)
- В) Двухфакторную аутентификацию
- Г) VPN-сервис

12. Что из перечисленного относится к психологическим (коммуникативным) рискам ребенка в цифровой среде?

- А) Заражение домашнего компьютера троянской программой
- Б) Кража пароля от аккаунта в онлайн-игре
- В) Вовлечение в закрытые деструктивные интернет-сообщества (например, суицидальной направленности)
- Г) Поломка экрана планшета во время урока

13. Первым действием классного руководителя при обнаружении факта жесткой травли ученика в классном чате должно быть:

- А) Немедленное удаление чата без сохранения переписки
- Б) Публичное высмеивание организатора травли перед всем классом
- В) Фиксация свидетельств (скриншоты), изоляция пострадавшего от нападок, информирование школьного психолога и администрации
- Г) Игнорирование ситуации (дети должны разобраться сами)

14. Психологическое состояние, характеризующееся навязчивым страхом пропустить интересное событие или важную новость в социальных сетях, называется:

- А) Синдром компьютерного зрения
- Б) Синдром упущенной выгоды (FoMO)
- В) Киберхондрия
- Г) Цифровой детокс

Раздел 3. Технологии проектирования и методики защиты цифровой среды

15. Какое из перечисленных правил является главным элементом парольной политики (цифровой гигиены) для учителя?

- А) Использование одного простого пароля (например, «123456») для всех рабочих и личных аккаунтов
- Б) Хранение записки с паролем на рамке школьного монитора
- В) Использование сложных, уникальных паролей для разных систем и включение двухфакторной аутентификации (2FA)
- Г) Передача своего пароля от электронного журнала старосте класса для выставления оценок

16. При проектировании безопасной ЦОС класса учитель отбирает цифровой контент. Какому источнику согласно ФГОС ОО следует отдать приоритет?

- А) Любому видеоролику с открытого видеохостинга YouTube по теме урока
- Б) Статье из Википедии, отредактированной неизвестным пользователем
- В) Верифицированным материалам из Библиотеки цифрового образовательного контента (ЦОК) Минпросвещения РФ
- Г) Презентации, скачанной со случайного форума взаимопомощи учителей

17. Использование концепции BYOD (Bring Your Own Device — «принеси свое устройство») в проектировании образовательного процесса означает:

- А) Запрет на любые технические устройства в здании школы
- Б) Использование личных гаджетов учащихся (планшеты, ноутбуки) для выполнения учебных задач под контролем педагога
- В) Обязательную покупку школой одинаковых планшетов для каждого ученика
- Г) Проведение уроков исключительно в компьютерном классе

18. Для проведения эффективного родительского собрания по теме «Безопасный интернет дома» педагогу целесообразно подготовить материал о:

- А) Настройке корпоративных брандмауэров Cisco
- Б) Программах и встроенных функциях родительского контроля на устройствах детей
- В) Языках программирования для создания сайтов
- Г) Способах обхода блокировок Роскомнадзора

19. Какой методический прием наиболее эффективен для формирования навыков цифровой гигиены у учащихся начальных классов?

- А) Чтение лекции по информационной безопасности в течение 45 минут
- Б) Интерактивная игра-квест «Путешествие по безопасному интернету» с разбором сказочных сюжетов
- В) Заучивание наизусть статей Уголовного кодекса РФ о киберпреступности
- Г) Полный запрет на обсуждение компьютеров в школе

20. В рамках управления рисками (УК-2) при планировании групповой работы школьников в облачном текстовом редакторе учитель в первую очередь должен:

- А) Назначить доступ «Редактировать всем, у кого есть ссылка» в открытом доступе в интернете
- Б) Настроить доступ по приглашениям (аккаунтам) только для участников рабочей группы и ограничить внешнюю публикацию документов
- В) Отказаться от использования облачных технологий
- Г) Проверить скорость печати каждого ученика

21. Резервное копирование (бэкап) методических материалов и цифровых проектов учащихся — это технологическая мера, направленная на защиту от:

- А) Кибербуллинга и оскорблений
- Б) Потери или уничтожения информации в результате технических сбоев или вирусных атак
- В) Фишинговых писем
- Г) Проникновения деструктивного контента в классные чаты

Критерии оценки:

Количество вопросов в тесте 21:

Оценка «5»- от 18-21 правильных ответов.

Оценка «4»- от 12-17 правильных ответов.

Оценка «3»- от 9-11 правильных ответов.

Оценка «2»- менее 9 правильных ответов.

7.2.4.Бально-рейтинговая система оценки знаний бакалавров

Согласно Положения о бально-рейтинговой системе оценки знаний бакалавров баллы выставляются в соответствующих графах журнала (см. «Журнал учета бально-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 бально-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 бальных 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 (п) 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 "незачтено". 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. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 5-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2026. — 384 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/02005-0>. - ISBN 978-5-369-02005-0. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2233509> . – Режим доступа: по подписке.
2. Безопасная образовательная среда: моделирование, проектирование, диагностика : учебно-методическое пособие / составители И. В. Непрокина [и др.]. — Тольятти : ТГУ, 2020. — 75 с. — ISBN 978-5-8259-1533-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/167146> . — Режим доступа: для авториз. пользователей..
3. Блинова, Е. Е. Цифровые технологии в образовании (Digital Technologies in Education) : билингвальное учебное пособие / Е. Е. Блинова, А. Г. Евланова ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2024. - 173 с. – ISBN 978-5-9275-4642-8. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2220015> . – Режим доступа: по подписке.
4. Федотова, Е. Л. Информационные технологии в науке и образовании : учебное пособие / Е.Л. Федотова, А.А. Федотов. — Москва : ФОРУМ : ИНФРА-М, 2024. — 335 с. — (Высшее образование). - ISBN 978-5-8199-0884-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2116864> . – Режим доступа: по подписке.
5. Цифровые технологии в педагогической деятельности : учебное пособие / А.А. Кузнецов, К.Е. Агафонова, К.Т. Юсупова [и др.]. — Москва : ИНФРА-М, 2025. — 223 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI 10.12737/2139201. - ISBN 978-5-16-019825-5. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2139201> . – Режим доступа: по подписке.

8.2. Дополнительная литература:

1. Потемкина, Т. В. Педагогическое проектирование в цифровой образовательной среде : учебное пособие / Т. В. Потемкина. - Москва : Издательский Дом НИТУ «МИСиС», 2021. - 72 с. - ISBN 978-5-907227-29-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1915736> . – Режим доступа: по подписке.

2. Избранные вопросы цифровой трансформации образования : монография / под ред. Л.Л. Босовой, Ю.В. Вайнштейн, В.В. Гриншука. — Москва : ИНФРА-М, 2024. — 188 с. — (Научная мысль). - ISBN 978-5-16-019938-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2146204> .
3. Информационно-психологическая безопасность: профилактика кибербуллинга в современной образовательной среде : монография / Н. С. Бобровникова, С. В. Пазухина, Т. И. Куликова [и др.]. - Чебоксары : Среда, 2025. - 217 с. - ISBN 978-5-908083-01-0. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2253863> .

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 вопросов, терминов, материала, вызывающего трудности. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Конспектирование источников. Работа с конспектом лекций, 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 семинарского типа. Изучение нового материала до его изложения на занятиях. Поиск, изучение и презентация информации по заданной теме, анализ научных источников. Самостоятельное изучение отдельных вопросов тем дисциплины, не рассматриваемых на занятиях лекционного и семинарского типа. Подготовка к текущему контролю, к промежуточной аттестации.
Подготовка к зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

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

10.1. Общесистемные требования

Электронная информационно-образовательная среда ФГБОУ ВО «КЧГУ»

<http://kchgu.ru>- адрес официального сайта университета

<https://do.kchgu.ru>- электронная информационно-образовательная среда КЧГУ

Электронно-библиотечные системы (электронные библиотеки)

Учебный год	Наименование документа с указанием реквизитов	Срок действия документа
-------------	---	-------------------------

2026-2027 учебный год	Электронно-библиотечная система ООО «Знаниум». Договор № 332 эбс с 02.06.2026г. Электронный адрес: https://znanium.com	С 02.06.2026г. до 01.06.2027г.
2026-2027 учебный год	Электронно-библиотечная система «Лань». Договор № 12 от 26.02.26г. Электронный адрес: https://e.lanbook.com	от 26.02.2026г. до 31.01.2027г.
2026-2027 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
2026-2027 учебный год	Национальная электронная библиотека (НЭБ). Договор №101/НЭБ/1391-п от 22. 02. 2023 г. Электронный адрес: http://rusneb.ru	Бессрочный
2026-2027 учебный год	Научная электронная библиотека «ELIBRARY.RU». Лицензионное соглашение №15646 от 21.10.2016 г. Электронный адрес: http://elibrary.ru	Бессрочный
2026-2027 учебный год	Электронный ресурс Polpred.com Обзор СМИ. Соглашение. Бесплатно. Электронный адрес: http://polpred.com	Бессрочный

10.2. 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/>

10.3. Необходимый комплект лицензионного программного обеспечения

- MicrosoftWindows (Лицензия № 60290784), бессрочная
- MicrosoftOffice (Лицензия № 60127446), бессрочная
- ABBY FineReader (лицензия № FCRP-1100-1002-3937), бессрочная
- CalculateLinux (внесён в ЕРПИ 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 07.03.2027 г.

10.4. 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 Elsevir <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>.

11. Особенности реализации дисциплины для инвалидов и 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>.

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
Переутверждена ОП ВО. 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. Электронно-библиотечная система «Лань». Договор № 10 от 11.02.2025. 4. Электронно-библиотечная система «Лань». Договор № 12 от 26.02.26г. Действует до 31.01.2027г. 5. Договор № 238 эбс ООО «Знаниум» от 23.04.2024г. Действует до 11 мая 2025г. 6. Договор № 249-эбс ООО «Знаниум» от 14.05.2025г. Действует до 14.05.2026г. Переутверждена ОП ВО. Обновлены: учебный план, календарный учебный график, РПД, РПП, программы ГИА, воспитания календарный план воспитательной работы. Обновлен договор №332 эбс ООО «Знаниум» от 02.06.2026г. Действует с 02.06.2026г. до 01.06.2027г.		30.04.2025г., протокол № 8 29.04.2026г., протокол № 7 03.06.2026г., протокол № 8	30.04.2025г. 29.04.2026г. 03.06.2026г.