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
Декан Р.А. Бостанов
«04» июля 2023 г.

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

Очная, очно-заочная, заочная

Год начала подготовки

2023

Карачаевск, 2023

Составитель: старший преподаватель кафедры ИВМ *Аргуянова А. Б.*

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 2023 - 2024 учебный год

Протокол № 11 от 03.07.2023 г.

Заведующий кафедрой, канд. физ.- мат. наук, доцент  /Шунгаров Х.Д./

СОДЕРЖАНИЕ

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.

		задач. УК-2.3. Использует инструменты и техники цифрового моделирования для реализации образовательных процессов	**Владеть:** навыками использования методов организации и контроля функционирования системы защиты информации; навыками использования стандартов для защиты информации в информационной системе.
ОПК-9	ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-9.1. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-9.2. Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности	**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. **Уметь:** пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения. **Владеть:** методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.
ПК-1	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 методы, приемы и технологии обучения, в том числе информационные	**Знать:** структуру, состав и дидактические единицы предметной области (преподаваемого предмета) **Уметь:** осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО **Владеть:** умением разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные

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.

Объём дисциплины	Всего часов		Всего часов
	для очной формы обучения	Для очно-заочной формы обучения	для заочной формы обучения
Общая трудоемкость дисциплины	108	108	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)	54	44	
Аудиторная работа (всего):	54	44	8
в том числе:			
лекции	36	14	2
семинары, практические занятия	18	30	6
практикумы	Не предусмотрено	Не предусмотрено	Не предусмотрено
лабораторные работы	Не предусмотрено	Не предусмотрено	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)	54	28	92
Контроль самостоятельной работы		36	8
Вид промежуточной аттестации обучающегося (зачет / экзамен)	Экзамен- 5 семестр	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 очной формы обучения

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

	основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. */лз/*							
2	Защита документов MS Office /п*р/*	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				8	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/*	4	4				УК-2 ОПК-9 ПК-1	Блиц-опрос
5	Тема: Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). /*пр*/	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				8	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/*	4	4				УК-2 ОПК-9 ПК-1	Устный опрос
8	Тема: Базовые методы криптографического преобразования данных. /п*р/*	2		2			УК-2 ОПК-9 ПК-1	Отчет по прак.работе
9	Тема: Программно-	4	4				УК-2	Блиц опрос

	технический уровень обеспечения защиты информации */лз/*						ОПК-9 ПК-1	
10	Тема: Использование методов замены для шифрования данных. /*пр*/	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.	**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*/	4	4				УК-2 ОПК-9 ПК-1	Фронтальный опрос
13	Тема: Классические шифры перестановки/*пр*/	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/*	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. /*лз/*	4	4				УК-2 ОПК-9 ПК-1	Тест по теме
16	Тема: Методы криптоанализа классических шифров. /*пр*/	2		2			УК-2 ОПК-9 ПК-1	Отчет по прак.работе
17	Тема: Обеспечение режима конфиденциальности при работе с защищаемой информацией. */ср/*	8				8	УК-2 ОПК-9 ПК-1	Реферат
18	Тема: Контроль за соблюдением требований информационной безопасности и защиты информации. /*лз/*	4	4				УК-2 ОПК-9 ПК-1	Фронтальный опрос
19	Тема: Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа. /*пр*/	4		4			УК-2 ОПК-9 ПК-1	Доклад с презентацией

20	Тема: Ответственность за правонарушения информационной безопасности и защиты информации. */ср/*	8				8	УК-2 ОПК-9 ПК-1	Вопросы к зачету
21	Тема: Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. /*лз/*	4	4				УК-2 ОПК-9 ПК-1	Блиц опрос
22	Тема: Уголовная ответственность за правонарушения в области защиты государственной тайны. /*лз/*	4	4				УК-2 ОПК-9 ПК-1	Устный опрос
23	Тема: Уголовная ответственность за правонарушения в области конфиденциальной информации. */ср/*	6				6	УК-2 ОПК-9 ПК-1	Реферат
	Всего	**108**	**36**	**18**		**54**		

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)					
		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**	**8**	**6**		**16**		
1	Тема: Необходимость и значимость нормативно-правового определения основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. */лз/*	4	2	2			УК-2 ОПК-9 ПК-1	Устный опрос
2	Защита документов MS Office /п*р/*	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/*	6				6	УК-2 ОПК-9 ПК-1	Вопросы к зачету
4	Тема: Основные угрозы информационной	2	2				УК-2 ОПК-9	Блиц-опрос

	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/*						ПК-1	
5	Тема: Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). /*пр*/	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. /п*р*/	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 шифрования данных. /*пр*/	2		2			УК-2 ОПК-9 ПК-1	Отчет по прак.работе
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	2	2				УК-2 ОПК-9 ПК-1	Фронтальный опрос

	системы защиты информации. /*лз*/							
13	Тема: Классические шифры перестановки/*пр*/	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. /*пр*/	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. /*пр*/	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 ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. /*лз/*	2		2			УК-2 ОПК-9 ПК-1	Блиц опрос
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 /п*р/*	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				8	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. */ср/*	4				4	УК-2 ОПК-9 ПК-1	Блиц-опрос
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	10				10	УК-2	Реферат

	защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз. */ср/*						ОПК-9 ПК-1	
	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 шифры перестановки/*пр*/	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/*	8				8	УК-2 ОПК-9 ПК-1	Вопросы к зачету
15	Тема: Структура систем защиты информации на современном этапе. Методы (виды)	4				4	УК-2 ОПК-9 ПК-1	Тест по теме

	обеспечения защиты информации. */ср/*							
16	Тема: Методы криптоанализа классических шифров. */ср/*	2				2	УК-2 ОПК-9 ПК-1	Отчет по прак.работе
17	Тема: Обеспечение режима конфиденциальности при работе с защищаемой информацией. */ср/*	8				8	УК-2 ОПК-9 ПК-1	Реферат
18	Тема: Контроль за соблюдением требований информационной безопасности и защиты информации. */ср/*	4				4	УК-2 ОПК-9 ПК-1	Фронтальный опрос
19	Тема: Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа. */ср/*	4				4	УК-2 ОПК-9 ПК-1	Доклад с презентацией
20	Тема: Ответственность за правонарушения информационной безопасности и защиты информации. */ср/*	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. */ср/*	4				4	УК-2 ОПК-9 ПК-1	Блиц опрос
22	Тема: Уголовная ответственность за правонарушения в области защиты государственной тайны. */ср/*	4				4	УК-2 ОПК-9 ПК-1	Устный опрос
23	Тема: Уголовная ответственность за правонарушения в области конфиденциальной информации. */ср/*	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. 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 лабораторных занятий. Инновационные образовательные технологии используются в процессе аудиторных занятий и самостоятельной работы студентов в виде применения активных и интерактивных методов обучения.

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

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

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

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

1. Обсуждение в группах

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

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

Преподаватель может устанавливать определенные правила проведения группового обсуждения:

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

-ввести алгоритм выработки общего мнения (решения);

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

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

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

2. Публичная презентация проекта

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

3. Дискуссия

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

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

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

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

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

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

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

7.1. Описание шкал оценивания степени сформированности компетенций

Уровни сформированности компетенций	Индикаторы	Качественные критерии оценивание			
		2 балла	3 балла	4 балла	5 баллов
УК-2					
Базовый	**Знать:** основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации; содержание основных уровней обеспечения информационной безопасности.	Не знает основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации; содержание основных уровней обеспечения информационной безопасности.	В целом знает основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации; содержание основных уровней обеспечения информационной безопасности.	Знает 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	Не умеет выполнять анализ требований к системе защиты информации; выявлять угрозы информационной безопасности, обосновывать организационно-	В целом умеет выполнять анализ требований к системе защиты информации; выявлять угрозы информационной безопасности, обосновывать организационно-	Умеет уверенно выполнять анализ требований к системе защиты информации; выявлять угрозы информационной безопасности, обосновывать организационно-	

	организационно-технические мероприятия по защите информации в информационной системе.	технические мероприятия по защите информации в информационной системе.	технические мероприятия по защите информации в информационной системе.	технические мероприятия по защите информации в информационной системе.	
	Владеть: навыками использования методов организации и контроля функционирования системы защиты информации; навыками использования стандартов для защиты информации в информационной системе	Не владеет навыками использования методов организации и контроля функционирования системы защиты информации; навыками использования стандартов для защиты информации в информационной системе	В целом владеет навыками использования методов организации и контроля функционирования системы защиты информации; навыками использования стандартов для защиты информации в информационной системе	Владеет навыками использования методов организации и контроля функционирования системы защиты информации; навыками использования стандартов для защиты информации в информационной системе	
Повышенный	**Знать:** основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации; содержание основных уровней обеспечения информационной безопасности.				В полном объеме знает 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.				Умеет в полном объеме выполнять анализ требований к системе защиты информации; выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационной системе.
	Владеть: навыками использования				В полном объеме владеет навыками использования

	методов организации и контроля функционирования системы защиты информации; навыками использования стандартов для защиты информации в информационной системе				методов организации и контроля функционирования системы защиты информации; навыками использования стандартов для защиты информации в информационной системе
			ОПК-9		
Базовый	**Знать:** основные 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.	Не знает основные 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.	В целом знает основные 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.	Знает основные 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.	
	Уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения.	Не умеет пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения.	В целом умеет пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения.	Умеет пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения.	
	Владеть: методами и средствами технической	Не владеет методами и средствами технической	В целом владеет методами и средствами технической	Владеет методами и средствами технической защиты	

	защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.	защиты информации; методами расчета и инструментального контроля показателей технической защиты информации. таблиц.	защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.	информации; методами расчета и инструментального контроля показателей технической защиты информации.	
Повышенный	**Знать:** основные 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				В полном объеме владеет основными средствами и методами 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
	Уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения.				В полном объеме пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения.
	Владеть: методами и средствами технической защиты информации; методами расчета и				В полном объеме владеет методами и средствами технической защиты информации; методами расчета и

	инструментального контроля показателей технической защиты информации.				инструментального контроля показателей технической защиты информации.

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:

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?

Критерии оценки устного ответа на вопросы по дисциплине «Методы и средства защиты информации»:

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

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

✓ 3 балла – фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной

литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.

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

7.2.3. Тестовые задания для проверки знаний студентов

УК-2

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

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

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

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

3) Виды информационной безопасности:

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

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

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

5) Основные объекты информационной безопасности:

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

6) Основными рисками информационной безопасности являются:

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

7) К основным принципам обеспечения информационной безопасности относится:

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

8) Основными субъектами информационной безопасности являются:

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

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

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

10) Принципом информационной безопасности является принцип недопущения:

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

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

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

12) Принципом политики информационной безопасности является принцип:

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

13) Принципом политики информационной безопасности является принцип:

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

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

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

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

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

16) Принцип Кирхгофа:

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

17) ЭЦП – это:

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

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

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

19) Наиболее распространены угрозы информационной безопасности сети:

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

20) Наиболее распространены средства воздействия на сеть офиса:

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

21) Утечкой информации в системе называется ситуация, характеризуемая:

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

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

+ Целостность
- Доступность
- Актуальность

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

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

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

- Регламентированной

- Правовой
+ Защищаемой

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

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

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

+ Владелец сети
- Администратор сети
- Пользователь сети

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

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

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

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

Методические материалы, определяющие процедуры оценивания знаний

Ключи к тестовым заданиям.

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

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

Критерии оценки тестового материала по дисциплине
«Методы и средства защиты информации»:

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

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

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

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

7.2.4. Балльно-рейтинговая система оценки знаний бакалавров

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

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

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

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

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

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

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

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

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

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

Таблица перевода балльно-рейтинговых показателей в отметки традиционной системы оценивания

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

Необходимое количество баллов для выставления отметок («зачтено», «удовлетворительно», «хорошо», «отлично») определяется произведением реально проведенных аудиторных часов (n) за отчетный период на коэффициент соответствия в

зависимости от соотношения часов лекционных и практических занятий согласно приведенной таблице.

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

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

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

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

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

8.1. Основная литература:

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

2. Башлы, П. Н. Информационная безопасность и защита информации : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222с. - ISBN 978-5-369-01178-2. - URL: https://znanium.com /catalog /product /405000

3. Баранова, Е. К. Основы информатики и защиты информации: учебное пособие / Е.К. Баранова Е.К. - М.: РИОР, ИНФРА-М, 2018. - 183 с. - ISBN 978-5-369-01169-0. - URL: https://znanium.com/catalog/ product /959916

4. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Москва: РИОР: ИНФРА-М, 2020. - 336 с. - ISBN 978-5-369-01761-6. - URL: https://znanium.com/catalog/product/1114032

8.2. Дополнительная литература:

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

2. Информационная безопасность и защита информации: учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов; Государственный университет «Дубна». - Дубна: Государственный университет «Дубна», 2020. - 85 с. - ISBN 978-5-89847-608-3. URL: https: //e.lanbook. com /book /154490

3. Криптографическая защита информации: учебное пособие / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.] ; под редакцией С. О. Крамарова. - Москва: РИОР: ИНФРА-М, 2021. - 321 с. - ISBN 978-5-369-01716-6. - URL: https://znanium.com/catalog/product /1153156

4. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. — 3-е изд., испр. и доп. - Москва : ИНФРА-М, 2020. — 327 с. . - ISBN 978-5-16-015471-8. - URL: https: //znanium.com /catalog /product /1035570

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

Вид учебных занятий	Организация деятельности студента
Лекция	Написание конспекта лекций: краткое, схематичное, последовательное фиксирование основных положений, выводов, формулировок, обобщений; выделение ключевых слов, терминов. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросы, терминов, материала, вызывающего трудности. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Выполнение всего объема самостоятельной подготовки, указанный в описаниях соответствующих практических работ; выполнение каждой работы предшествует проверка готовности студента, которая проводится преподавателем; представление отчета о проделанной работе с обсуждением полученных результатов и выводов.
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 экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

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

10.1. Общесистемные требования

Электронная информационно-образовательная среда ФГБОУ ВО «КЧГУ»

http://kchgu.ru - адрес официального сайта университета
https://do.kchgu.ru - электронная информационно-образовательная среда КЧГУ

Электронно-библиотечные системы (электронные библиотеки)

Учебный год	Наименование документа с указанием реквизитов	Срок действия документа
2022 / 2023 учебный год	Электронно-библиотечная система ООО «Знаниум». Договор № 179 ЭБС от 22.03.2022г	с 30.03.2022 г по 30.03.2023 г.
	Электронно-библиотечная система «Лань». Договор № СЭБ НВ-294 от 1 декабря 2020 года.	Бессрочный
2022 /2023 учебный год	Электронная библиотека КЧГУ (Э.Б.).Положение об ЭБ утверждено Ученым советом от 30.09.2015г.Протокол № 1). Электронный адрес: https: kchgu.ru/biblioteka - kchgu/	Бессрочный

2022 / 2023 учебный год	Электронно-библиотечные системы: Научная электронная библиотека «ELIBRARY.RU» - https://www.elibrary.ru. Лицензионное соглашение №15646 от 01.08.2014г.Бесплатно. Национальная электронная библиотека (НЭБ) – https://rusneb.ru. Договор №101/НЭБ/1391 от 22.03.2016г.Бесплатно. . Электронный ресурс «Polred.com Обзор СМИ» – https://polpred.com. Соглашение. Бесплатно.	Бессрочно

10.2. Материально-техническое и учебно-методическое обеспечение дисциплины

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

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

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

Занятия проводятся в следующих аудиториях:

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1.Учебная аудитория для проведения занятий лекционного типа, практических и семинарских занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. 2.Для проведения конференций. *Специализированная мебель:* столы ученические, стулья, стол преподавателя, доска меловая. *Технические средства обучения*: ноутбук с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, телевизор, переносной проектор. *Лицензионное программное обеспечение:* Microsoft Windows (Лицензия № 60290784), бессрочная. Microsoft Office (Лицензия № 60127446), бессрочная Kaspersky Endpoint Security (Лицензия № 280E-210210-093403-420-2061), с 03.03.2021 по 04.03.2023г.	369200, Карачаево-Черкесская Республика, г. Карачаевск, ул. Ленина, 29. Учебный корпус №2, ауд. 13
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторных работ и курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. *Специализированная мебель:* столы ученические, стулья, стол преподавателя, маркерная доска. *Технические средства обучения:* 1) 10 персональных компьютеров с подключением к сети «Интернет» и обеспечением доступа в электронную	369200, Карачаево-Черкесская Республика, г. Карачаевск, ул. Ленина, 29. Учебный корпус №2, ауд. 20

информационно-образовательную среду университета. 2) Интерактивный комплекс: интерактивная доска, проектор с ноутбуком, звуковые колонки. *Лицензионное программное обеспечение:* Microsoft Windows (Лицензия № 60290784), бессрочная. Microsoft Office (Лицензия № 60127446) бессрочная. Kaspersky Endpoint Security (Лицензия № 280E-210210-093403-420-2061), с 03.03.2021 по 04.03.2023г. Пакет приложений для объектно-ориентированного программирования Embarcadero (Item Number: 2013123054325206). Бессрочная лицензия. Пакет визуального 3D-моделирования Blender (лицензия GNU GPL v3). Бессрочная лицензия. Векторный графический редактор Inkscape (лицензия GNU GPL v3). Бессрочная лицензия. Программный комплекс для верстки Scribus (лицензия GNU GPL v3). Бессрочная лицензия. Graphisoft ArchiCAD номер лицензии SOXXH-HXXXN-6XXNJ-0MXXX Учебная (бесплатная). Образовательная лицензия на период до 2021года включительно. Adobe Photoshop номер лицензии License RU (65170869). Бессрочная лицензия. Autodesk AutoCAD номер лицензии 5X6-30X999XX. Бессрочная образовательная (академическая) лицензия. Autodesk 3DS Max номер лицензии 5X5-93X928XX. Бессрочная образовательная (академическая) лицензия. Autodesk Revit номер лицензии 5X6-03X109XX. Бессрочная образовательная (академическая) лицензия. Corel DRAW номер лицензии LCCDGSX6MLCRA. Бессрочная лицензия. IBM SPSS Statistics Base, Custom Tables V22. Бессрочная лицензия.	

10.3. Необходимый комплект лицензионного программного обеспечения

1. ABBY FineReader (лицензия №FCRP-1100-1002-3937), бессрочная.
2. Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная.
3. GNU Image Manipulation Program (GIMP) (лицензия: №GNU GPLv3), бессрочная.
4. Google G Suite for Education (IC: 01i1p5u8), бессрочная.
5. Kaspersky Endpoint Security (лицензия №280E2102100934034202061), с 03.03.2021 по 04.03.2023 г.
6. Microsoft Office (лицензия №60127446), бессрочная.
7. Microsoft Windows (лицензия №60290784), бессрочная.

10.4. Современные профессиональные базы данных и информационные справочные системы

Современные профессиональные базы данных

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

Информационные справочные системы

1. Портал Федеральных государственных образовательных стандартов высшего образования - http://fgosvo.ru.

2. Федеральный центр информационно-образовательных ресурсов (ФЦИОР) – http://edu.ru.

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

4. Информационная система «Единое окно доступа к образовательным ресурсам» (ИС «Единое окно») – http://window/edu.ru.

5. Информационная система «Информио».

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

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

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

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

В группах, в состав которых входят обучающиеся с ОВЗ, в процессе учебных занятий используются технологии, направленные на диагностику уровня и темпов профессионального становления обучающихся с ОВЗ, а также технологии мониторинга степени успешности формирования у них компетенций, предусмотренных ФГОС ВО при изучении данной учебной дисциплины, используя с этой целью специальные оценочные материалы и формы проведения промежуточной и итоговой аттестации, специальные технические средства, предоставляя обучающимся с ОВЗ дополнительное время для подготовки ответов, привлекая тьютеров).

Материально-техническая база для реализации программы:

1.Мультимедийные средства:

- интерактивные доски «Smart Boarfd», «Toshiba»;
- экраны проекционные на штативе 280*120;
- мультимедиа-проекторы Epson, Benq, Mitsubishi, Aser;

2.Презентационное оборудование:

- радиосистемы AKG, Shure, Quik;
- видеокомплекты Microsoft, Logitech;
- микрофоны беспроводные;
- класс компьютерный мультимедийный на 21 мест;
- ноутбуки Aser, Toshiba, Asus, HP;

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

12. Лист регистрации изменений

Изменение	**Дата и номер протокола ученого совета факультета/ института, на котором были рассмотрены вопросы о необходимости внесения изменений в ОП ВО**	**Дата и номер протокола ученого совета Университета, на котором были утверждены изменения в ОП ВО**	**Дата введения изменения**