МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

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

Факультет экономики и управления

УТВЕРЖДАЮ
Декан _____ З.М. Чомаева
18.06.2022г.
М.П.

Рабочая программа дисциплины

Информационная безопасность
(наименование дисциплины (модуля)

Направление подготовки

09.03.03 Прикладная информатика

(шифр, название направления)

Направленность (профиль) подготовки

«Прикладная информатика в экономике»

Квалификация выпускника

бакалавр

Форма обучения

Очная / заочная

Год начала подготовки - 2020
(по учебному плану)

Карачаевск, 2023

Программу составил(а): *канд. экон. наук, доцент Маршанов Б.М.*

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 922 «Об утверждении федерального государственного образовательного стандарта высшего образования» - бакалавриат по направлению подготовки 09.03.03 «Прикладная информатика» с изменениями и дополнениями от 8 февраля 2021 г., образовательной программой высшего образования по направлению подготовки 09.03.03 Прикладная информатика, профиль – Прикладная информатика в экономике; локальными актами КЧГУ.

Рабочая программа обновлена и утверждена на заседании кафедры экономики и прикладной информатики на 2023-2024 уч. год

Протокол № 10.2 от 22. 06. 2023 г.

И.о. заведующего кафедрой _____*канд. экон. наук, доцент Маршанов Б.М.*

СОДЕРЖАНИЕ

1. Наименование дисциплины (модуля)

Информационная безопасность

Целью изучения дисциплины является: сформировать у студентов готовность обеспечивать информационную безопасность и систему защиты информации в современном информационном обществе и способность соблюдать основные требования информационной безопасности.

Для достижения цели ставятся задачи:

– овладеть теоретическими, практическими и методическими вопросами обеспечения информационной безопасности;

– освоить методы защиты информации от различных видов объективных и субъективных угроз в процессе их возникновения, обработки, использования и хранения;

– формировать умение применять на практике полученные знания.

2. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина (модуль) относится к Блоку 1 и реализуется в рамках базовой части Б.1.

Дисциплина (модуль) изучается на 3 курсе в 5 и 6 семестрах очной формы обучения и на 4 курсе в 7-8 семестрах заочной формы обучения.

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП	
Индекс	Б1.О.20
Требования к предварительной подготовке обучающегося:	
Для успешного освоения дисциплины студент должен иметь базовую подготовку по таким дисциплинам как: «Математический анализ», «Линейная алгебра», «Информатика и программирование», в объёме изучаемой программы бакалавриата по направлению «Прикладная информатика»	
Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Курс "Информационная безопасность" является основой для последующего изучения таких дисциплин как: «Электронный документооборот»; «Информационные системы управления», «Управление информационными системами». Также, полученные знания в процессе изучения дисциплины, позволят успешно пройти все виды практик.	

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

В результате освоения ОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

Код компетенций	Содержание компетенции в соответствии с ФГОС ВО/ ПООП/ ООП	Индикаторы достижения компетенций	Декомпозиция компетенций (результаты обучения) в соответствии с установленными индикаторами
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе	**знать:** основы предметной области: основные разделы информационной безопасности: об информации, методах ее хранения, обработки и

	культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	передачи; об основных алгоритмах обработки информации и их сложности; об архитектуре вычислительной системы и принципах её функционирования; свойства информации, определяющие выбор средств и методов информационной защиты и влияющие на ее результативность работать с научной литературой и другими источниками научно-технической информации: правильно понимать смысл текстов, описывающих методы и модели в профессиональной сфере; **уметь:** работать с конспектами, учебником, учебно-методической, справочной литературой, другими источниками информации; воспринимать и осмысливать информацию развиваемых направлений информационной защиты; применять полученные знания для решения учебных задач; наиболее распространённые цели, способы и мотивы совершения преступлений с использованием компьютерных технологий; о методах и средствах обеспечения защиты информационной безопасности личности и общества. **владеть:** культурой мышления: способен к

			обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения составы преступлений в сфере компьютерной информации, предусмотренные УК РФ, и толкование специальных терминов, употребляемых в них.
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла	**Знать:** основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности. **Уметь:** применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности. **Владеть:** навыками составления технической документации на различных этапах жизненного цикла и систем обеспечения информационной безопасности.

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 **4 ЗЕТ, 144** академических часов.

Объём дисциплины	Всего часов

	для очной формы обучения	для заочной формы обучения
Общая трудоёмкость дисциплины	144	144
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)	72	16
Аудиторная работа (всего):	72	16
в том числе:		
лекции	36	8
семинары, практические занятия	36	8
практикумы		
лабораторные работы		
Внеаудиторная работа:		
курсовые работы		
консультация перед экзаменом		
Внеаудиторная работа также включает индивидуальную работу обучающихся с преподавателем, групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем), творческую работу (эссе), рефераты, контрольные работы и д		
Самостоятельная работа обучающихся (всего)	72	120
Контроль самостоятельной работы		8
Вид промежуточной аттестации обучающегося (зачет / экзамен)	зачет, 4,5 сем	зачет, 7,8 сем

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. Основы информационной безопасности**							
2.	Понятие информационной безопасности. Основные составляющие. Определите основные	8	2	2		4	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания

	аспекты актуальности информационной безопасности в современный период. Понятия о видах вирусов.							
3.	Наиболее распространённые угрозы. Основные определения и критерии классификации угроз. Правовая и техническая защита информации. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».\	8	2	2		4	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
4.	Законодательный уровень информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	16	4	4		8	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
5.	Стандарты и спецификации в области информационной безопасности. Основные положения теории информационной безопасности информационных систем.	8	2	2		4	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
6.	Административный уровень информационной безопасности.	8	2	2		4	ОПК-3, ОПК-4	Устный опрос, тест, проверка

	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства							практического задания
7.	Управление рисками. Этапы управления рисками. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	8	2	2		4	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
8.	Процедурный уровень информационной безопасности. Физическая защита. Реагирование на нарушения режима безопасности.	16	4	4		8	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
9.	**Раздел 2. Методы защиты информации**							
10.	Основные программно-технические меры. Методы криптографии. Защита программ от несанкционированной эксплуатации за счет привязки к носителю информации.	16	4	4		8	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
11.	Идентификация и аутентификация, управление доступом. Использование защищенных компьютерных систем. Основные положения теории информационной безопасности информационных систем.	16	4	4		8	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
12.	Протоколирование и аудит, шифрование, контроль,	16	4	4		8	ОПК-3, ОПК-4	Устный опрос, тест, проверка

	целостности. Защита информации от утечки по техническим причинам.							практического задания
13.	Экранирование, анализ защищенности. Международные стандарты информационного обмена. Понятие угрозы.	16	4	4		8	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
14.	Обеспечение высокой доступности. Туннелирование и управление. Важность и сложность проблемы информационной безопасности.	8	2	2		4	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
15.	Итого	**144**	**36**	**36**		**72**		

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			
1.	**Раздел 1. Основы информационной безопасности**							
2.	Понятие информационной безопасности. Основные составляющие. Определите основные аспекты актуальности информационной безопасности в современный период. Понятия о видах вирусов.	8	2			6	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
3.	Наиболее распространённые угрозы. Основные определения и	8		2		6	ОПК-3, ОПК-4	Устный опрос, тест, проверка

	критерии классификации угроз. Правовая и техническая защита информации. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».\							практического задания
4.	Законодательный уровень информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	14	2			12	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
5.	Стандарты и спецификации в области информационной безопасности. Основные положения теории информационной безопасности информационных систем.	8		2		6	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
6.	Административный уровень информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	8				8	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
7.	Управление рисками. Этапы управления рисками. Таксономия нарушений	8				8	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания

	информационной безопасности вычислительной системы и причины, обуславливающие их существование.							
8.	Процедурный уровень информационной безопасности. Физическая защита. Реагирование на нарушения режима безопасности.	14				14	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
9.	Контроль	4				4		
10.	**Раздел 2. Методы защиты информации**							
11.	Основные программно-технические меры. Методы криптографии. Защита программ от несанкционированной эксплуатации за счет привязки к носителю информации.	12	2			10	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
12.	Идентификация и аутентификация, управление доступом. Использование защищенных компьютерных систем. Основные положения теории информационной безопасности информационных систем.	12		2		10	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
13.	Протоколирование и аудит, шифрование, контроль, целостности. Защита информации от утечки по техническим причинам.	12	2			10	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
14.	Экранирование, анализ защищенности. Международные стандарты	12		2		10	ОПК-3, ОПК-4	Устный опрос, тест, проверка

	информационного обмена. Понятие угрозы.							практического задания
15.	Обеспечение высокой доступности. Туннелирование и управление. Важность и сложность проблемы информационной безопасности.	16				16	ОПК-3, ОПК-4	Устный опрос, тест, проверка практического задания
16.	Контроль	8						
17.	Итого	**144**	**8**	**8**		**120**		

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.

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 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 развёрнутый 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.

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

7.1. *Описание шкал оценивания степени сформированности компетенций*

Уровни сформированности компетенций	Индикаторы	Качественные критерии оценивание			
		2 балла	3 балла	4 балла	5 баллов
ОПК-3					
Базовый	**Знать:** основы предметной области: основные разделы информационной безопасности: об информации, методах ее хранения, обработки и передачи; об основных алгоритмах обработки информации и их сложности; об архитектуре вычислительной системы и принципах её функционирования; свойства информации, определяющие выбор средств и методов информационн	Не знает основы предметной области: основные разделы информационной безопасности: об информации, методах ее хранения, обработки и передачи; об основных алгоритмах обработки информации и их сложности; об архитектуре вычислительной системы и принципах её функционирования; свойства информации, определяющие выбор средств и методов	В целом знает основы предметной области: основные разделы информационной безопасности: об информации, методах ее хранения, обработки и передачи; об основных алгоритмах обработки информации и их сложности; об архитектуре вычислительной системы и принципах её функционирования; свойства информации, определяющие выбор средств и методов	Знает основы предметной области: основные разделы информационной безопасности: об информации, методах ее хранения, обработки и передачи; об основных алгоритмах обработки информации и их сложности; об архитектуре вычислительной системы и принципах её функционирования; свойства информации, определяющие выбор средств и методов информационн	

	ой защиты и влияющие на ее результативность работать с научной литературой и другими источниками научно-технической информации: правильно понимать смысл текстов, описывающих методы и модели в профессиональной сфере.	информационной защиты и влияющие на ее результативность работать с научной литературой и другими источниками научно-технической информации: правильно понимать смысл текстов, описывающих методы и модели в профессиональной сфере.	информационной защиты и влияющие на ее результативность работать с научной литературой и другими источниками научно-технической информации: правильно понимать смысл текстов, описывающих методы и модели в профессиональной сфере.	ой защиты и влияющие на ее результативность работать с научной литературой и другими источниками научно-технической информации: правильно понимать смысл текстов, описывающих методы и модели в профессиональной сфере.	
	Уметь: работать с конспектами, учебником, учебно-методической , справочной литературой, другими источниками информации; воспринимать и осмысливать информацию развиваемых направлений информационной защиты; применять полученные знания для решения учебных задач; наиболее распространенные цели, способы и мотивы совершения преступлений с	Не умеет работать с конспектами, учебником, учебно-методической , справочной литературой, другими источниками информации; воспринимать и осмысливать информацию развиваемых направлений информационной защиты; применять полученные знания для решения учебных задач; наиболее распространенные цели, способы и мотивы совершения преступлений	В целом умеет работать с конспектами, учебником, учебно-методической , справочной литературой, другими источниками информации; воспринимать и осмысливать информацию развиваемых направлений информационной защиты; применять полученные знания для решения учебных задач; наиболее распространенные цели, способы и мотивы совершения преступлений	Умеет работать с конспектами, учебником, учебно-методической , справочной литературой, другими источниками информации; воспринимать и осмысливать информацию развиваемых направлений информационной защиты; применять полученные знания для решения учебных задач; наиболее распространенные цели, способы и мотивы совершения преступлений	

	использование м компьютерных технологий; о методах и средствах обеспечения защиты информационн ой безопасности личности и общества.	с использование м компьютерных технологий; о методах и средствах обеспечения защиты информационн ой безопасности личности и общества.	с использование м компьютерных технологий; о методах и средствах обеспечения защиты информационн ой безопасности личности и общества.	с использование м компьютерных технологий; о методах и средствах обеспечения защиты информационн ой безопасности личности и общества.	
	Владеть: культурой мышления: способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения составы преступлений в сфере компьютерной информации, предусмотренн ые УК РФ, и толкование специальных терминов, употребляемых в них.	Не владеет культурой мышления: способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения составы преступлений в сфере компьютерной информации, предусмотренн ые УК РФ, и толкование специальных терминов, употребляемы х в них.	В целом владеет культурой мышления: способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения составы преступлений в сфере компьютерной информации, предусмотренн ые УК РФ, и толкование специальных терминов, употребляемы х в них.	Владеет культурой мышления: способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения составы преступлений в сфере компьютерной информации, предусмотренн ые УК РФ, и толкование специальных терминов, употребляемы х в них.	
Повышен ный	**Знать:** основы предметной области: основные разделы информационн ой безопасности: об информации, методах ее хранения, обработки и				В полном объеме знает основы предметной области: основные разделы информационн ой безопасности: об информации, методах ее

	передачи; об основных алгоритмах обработки информации и их сложности; об архитектуре вычислительной системы и принципах её функционирования; свойства информации, определяющие выбор средств и методов информационной защиты и влияющие на ее результативность работать с научной литературой и другими источниками научно-технической информации: правильно понимать смысл текстов, описывающих методы и модели в профессиональной сфере.				хранения, обработки и передачи; об основных алгоритмах обработки информации и их сложности; об архитектуре вычислительной системы и принципах её функционирования; свойства информации, определяющие выбор средств и методов информационной защиты и влияющие на ее результативность работать с научной литературой и другими источниками научно-технической информации: правильно понимать смысл текстов, описывающих методы и модели в профессиональной сфере.
	Уметь: работать с конспектами, учебником, учебно-методической , справочной литературой, другими источниками информации; воспринимать				Умеет в полном объеме работать с конспектами, учебником, учебно-методической , справочной литературой, другими источниками

	и осмысливать информацию развиваемых направлений информационной защиты; применять полученные знания для решения учебных задач; наиболее распространенные цели, способы и мотивы совершения преступлений с использованием компьютерных технологий; о методах и средствах обеспечения защиты информационной безопасности личности и общества.				информации; воспринимать и осмысливать информацию развиваемых направлений информационной защиты; применять полученные знания для решения учебных задач; наиболее распространенные цели, способы и мотивы совершения преступлений с использованием компьютерных технологий; о методах и средствах обеспечения защиты информационной безопасности личности и общества.
	Владеть: культурой мышления: способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения составы преступлений в сфере компьютерной информации, предусмотренн				В полном объеме владеет культурой мышления: способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения составы преступлений в сфере компьютерной информации,

	ые УК РФ, и толкование специальных терминов, употребляемых в них.				предусмотренные УК РФ, и толкование специальных терминов, употребляемых в них.
ОПК-4					
Базовый	**Знать:** основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.	Не знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.	В целом знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.	Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.	
	Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.	Не умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.	В целом умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.	Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.	
	Владеть: навыками составления технической документации на различных этапах жизненного цикла и систем	Не владеет навыками составления технической документации на различных этапах жизненного цикла и систем	В целом владеет навыками составления технической документации на различных этапах жизненного	Владеет навыками составления технической документации на различных этапах жизненного цикла и систем	

	обеспечения информационной безопасности.	обеспечения информационной безопасности.	цикла и систем обеспечения информационной безопасности.	обеспечения информационной безопасности.	
Повышенный	**Знать:** основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.				В полном объеме знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.
	Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.				В полном объеме применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.
	Владеть: навыками составления технической документации на различных этапах жизненного цикла и систем обеспечения				В полном объеме владеет навыками составления технической документации на различных этапах жизненного

	информационной безопасности.				цикла и систем обеспечения информационной безопасности.

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. Роль информационного права и информационной безопасности в современном обществе.
2. Назначение и структура системы защиты информации коммерческого предприятия.
3. Термины и определения в области защиты информации.
4. Особенности работы с персоналом, владеющим конфиденциальной информацией.
5. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.
6. Система защиты информации в зарубежных странах.
7. Система защиты информации в банковских системах/ системах страхования.
8. Методика защиты информации в системах электронного документооборота. (Системы на выбор).
9. Возможные атаки на алгоритм DES.
10. Достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами.
11. Атаки, которые могут быть использованы при нападении на протоколы идентификации.
12. Назначение и структура сертификата открытого ключа.
13. Виды и состав угроз информационной безопасности.
14. Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты.
15. Функции секретаря-референта в области защиты конфиденциальной информации.
16. Защита информации в процессе переговоров и совещаний.
17. Методики отбора персонала для работы с конфиденциальной информацией.
18. Государственная тайна и порядок ее защиты.
19. Организация защиты авторских и смежных прав в РФ.
20. Направления и методы защиты профессиональной тайны.
21. Нотариальная тайна и порядок ее защиты.
22. Адвокатская тайна и порядок ее защиты.
23. Тайна страхования и порядок ее защиты.
24. Банковская тайна и порядок ее защиты.
25. Тайна почтовых отправлений и порядок ее защиты.
26. Направления и методы защиты служебной тайны.
27. Направления и методы защиты персональных данных о гражданах.
28. Методы защиты личной и семейной тайны.
29. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
30. Анализ источников, каналов распространения и каналов утечки информации.

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

1. Роль информации в современном мире.
2. Значение защиты информации и информационной безопасности.
3. Аспекты защиты информации. Анализ схем защиты информации.
4. Современная система удостоверяющих документов и её недостатки.
5. Бесперспективность защиты носителей. Практика выявления поддельных документов.
6. Организация защиты информации в вычислительном центре (ВЦ) крупного предприятия. Внешнее окружение ВЦ.
7. Способы контроля доступа к информации.
8. Применимость мер защиты. Надежность и восстановление ЭВМ.
9. Экономические проблемы ЗИ.
10. Меры противодействия и затраты на их организацию.
11. Понятия, относящиеся к защите ВС. Целостность ресурсов, защита ресурсов, право владения, надежность.
12. Защита вычислительной сети. Классификация вторжений.
13. Концепция защищенной ВС.
14. Защита объектов ВС.
15. Защита линий связи.
16. Защита баз данных.
17. Защита подсистемы управления ВС.
18. Классификация сбоев и нарушения прав доступа к информации.
19. Физическая защита кабельной системы.
20. Физическая защита систем электроснабжения.
21. Системы архивирования и дублирования информации.
22. Защита информации в операционных системах.
23. Защита информации в прикладном ПО.
24. Способы идентификации пользователей.

25. Основные механизмы проверки подлинности пароля.
26. Механизм проверки подлинности "рукопожатие".
27. Проблема защиты информации в распределенных сетях.
28. Брандмауеры. Основные понятия.
29. Межсетевой экран. Классификация межсетевых экранов.
30. Классификация компьютерных вирусов.
31. Структура файловых, резидентных вирусов и вирусов-червей.
32. Жизненный цикл компьютерных вирусов.
33. Способы и симптомы заражения вирусами.
34. Общая классификация средств защиты от вирусов.
35. Стандарт шифрования данных DES.
36. Асимметрические (открытые) криптосистемы.
37. Применение криптографии.
38. Основные направления компьютерных преступлений.

Критерии оценки устного ответа на вопросы по дисциплине «Информационная безопасность»:

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

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

✓ 3 балла – фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.

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

7.2.3. Тестовые задания для проверки знаний студентов

1. Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:

- **со стороны злоумышленника**
- со стороны законного отправителя сообщения
- со стороны законного получателя сообщения

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

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

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

- шифрование
- дешифровка
- **расшифровка**

4. В каких основных форматах существует симметричный алгоритм?
- блока и строки;
- **потока и блока;**
- потока и данных

5. Открытым текстом в криптографии называют:
- расшифрованный текст
- любое послание
- **исходное послание**

6. Какой ключ известен только приемнику?
- открытый
- **закрытый**

7. Наука, занимающаяся защитой информации, путем преобразования этой информации это:
- криптография
- **криптология**
- криптоанализ

8. В каких **шифрах результат шифрования очередного блока зависит только от** него самого и не зависит от других блоков шифруемого массива данных?
- в потоковых
- **в блочных**

9. Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:
- шифр функциональных преобразований
- шифр замен
- **шифр перестановок**

10. Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется:
- **функция шифрования шага преобразования**
- инвариант стандартного шага шифрования

11. Шифрование-это:
- процесс создания алгоритмов шифрования
- процесс сжатия информации
- **процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется**

12. В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией?
- **при шифровании с помощью ассимметричного алгоритма**

- при шифровании с помощью симметричного алгоритма
- арбитр необходим всегда

13. Можно ли отнести слабую аутентификацию к проблемам безопасности?
- нет
- **да**
- в редких случаях

14. Возможно ли расшифровывать информацию без знания ключа?
- нет
- **да**
- в редких случаях

15. Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый?
- **нет**
- да
- в редких случаях

16. Характерная черта алгоритма Эль-Гамаля состоит в :
- **протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя**
- в точной своевременной передаче сообщения
- алгоритм не имеет особенностей и идентичен RSA

17. Аутентификацией называют:
- процесс регистрации в системе
- способ защиты системы
- **процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов**

18. Аутентификация бывает:
- статическая
- устойчивая
- постоянная
- **все варианты правильные**
- правильного варианта нет

19. Стойкость ключа характеризуется
- длинной
- непредсказуемостью
- **все варианты правильные**
- правильного варианта нет

20. Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:
- **на основе произвольно выбранного шифротекста**
- **на основе произвольно выбранного открытого текста**
- на основе только шифротекста

21. **Условие,** при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им *массива открытых данных* размера n используется в анализе:

- **на основе произвольно выбранного шифротекста**
- **на основе произвольно выбранного открытого текста**
- правильного ответа нет

Задача №1

Вы – сотрудник лечебного учреждения. Ежедневно в базе данных происходит накопление большого количества информации.

1. Перечислите возможные способы способом обеспечения целостности и предотвращения уничтожения данных.

2. Определите, каким способом Вам необходимо воспользоваться. Объясните почему.

Решение:

1. Резервное копирование, архивирование.

2. В случае резервного копирования речь идет о кратко- или среднесрочном дополнительном хранении данных, которые еще могут понадобиться пользователям в их работе. Если, например, в результате повреждения жесткого диска или по иным причинам текущие данные теряются, их удастся быстро восстановить. Так можно эффективно защитить данные от разного рода случайностей. Время хранения резервных копий массива данных устанавливается не слишком продолжительное — несколько недель или месяцев.

Архивированию, напротив, подвергаются данные, которые из категории активно используемых перешли в «статичное» состояние, поэтому к ним обращаются сравнительно редко. Их можно уже извлечь из резервной копии и сохранить в архиве. Оба подхода различаются и уровнем затрат на приобретение необходимых технических средств: для архивирования большого объема данных применяются, как правило, недорогие носители с высокой емкостью хранения, например, оптические носители.

В описанной выше ситуации необходимо осуществлять резервное копирование данных.

Ответ: Резервное копирование, архивирование.

Задача №2:

Вы – руководитель отдела информационной безопасности организации. Вы подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

1. Какая статья уголовного кодекса была нарушена?

2. Какое наказание должен понести нарушитель?

Решение:

1. Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

2. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Ответ: 273ст.

Задача №3:

На доске объявлений размещено сообщение, в котором говорится о том, что каждому сотруднику организации выделяется персональный пароль. Для того чтобы сотрудники его не забыли, пароль представляет дату рождения и имя каждого сотрудника.

1. Какие правила обеспечения информационной безопасности нарушены?
2. Какие символы должны быть использованы при записи пароля?

Решение:

1. Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Ответ: пароли были раскрыты

Задача №4:

Вы руководитель отдела информационной безопасности организации. У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации.

1. Какая статья уголовного кодекса была нарушена?
2. Какое наказание должен понести нарушитель?

Решение:

1. Статья 272. Неправомерный доступ к компьютерной информации.

2. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

Ответ: ст.272 УК РФ

Задача №5:

Гражданин П. проник в информационную базу учебной организации и скопировал интересующую его информацию с ограниченным доступом, о чем стало известно администраторам информационной системы. Через неделю ему пришла повестка в суд.

1. Являются ли его действия противозаконными?
2. С чем это связано?
3. Какое наказание может ждать гражданина П. за совершенные им действия?

Решение:

1. Да.

2. Гражданин П. нарушил закон – Гл.28 УК РФ ст. 272 Неправомерный доступ к компьютерной информации.

3. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ

или их сети, наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

Ответ:

1.Да

2. ст.272 УК РФ

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

«Информационная безопасность»:

✓ 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. Бально-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 определённого 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 (модуля)

8.1. Основная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326

2. Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - ISBN 978-5-91612-276-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1094244

3. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013711

8.2. Дополнительная литература:

1. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184

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

3. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1137902

9 .Методические указания для обучающихся по освоению 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. Уделить внимание следующим понятиям (*перечисление понятий*) и др.
Практические занятия	Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом (*указать текст из источника и др.)*. Прослушивание аудио- и видеозаписей по заданной теме, решение расчетно-графических заданий, решение задач по алгоритму и др.
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.
Практикум / лабораторная работа	Методические указания по выполнению лабораторных работ (*можно указать название брошюры и где находится) и др.*
Коллоквиум	Работа с конспектом лекций, подготовка ответов к контрольным вопросам и др.
Подготовка к экзамену (зачету)	При подготовке к экзамену (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
2023 / 2024 учебный год	Договор №915 эбс ООО « Знаниум» от 12.05.2023г.	с 30.03.2022 г по 30.03.2023 г. протокол №10
	Электронно-библиотечная система «Лань». Договор № СЭБ НВ-294 от 1 декабря 2020 года.	Бессрочный
2023 / 2024 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
2023 / 2024 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

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 помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом**
Лаборатория информационных систем и технологии для проведения занятий лекционного типа, занятий лабораторного типа, занятий семинарского типа, практического типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. *Специализированная мебель:* *столы ученические, стулья, доска маркерная.* *Учебно-наглядные пособия (в электронном виде).* *Технические средства обучения:* Персональные компьютеры в количестве 20 шт. с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета. *Лицензионное программное обеспечение:* – Microsoft Windows (Лицензия № 60290784), бессрочная – Microsoft Office (Лицензия № 60127446), бессрочная – ABBY Fine Reader (лицензия № FCRP-1100-1002-3937), бессрочная – Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная – Google G Suite for Education (IC: 01i1p5u8), бессрочная – Антивирус Касперского. Действует до 03.03.2025г. (Договор № 56/2023 от 25 января 2023г.); – пакет приложений для объектно-ориентированного программирования Embarcadero (Item Number: 2013123054325206. Срок действия лицензии: бессрочная); – пакет визуального редактирования растровых изображений GIMP (Лицензия № GNU GPLv3. Срок действия лицензии: бессрочная); – образовательная подписка Google G Suite for Education (видеоконференции, дневник, календарь, диск и прочее). (Срок действия лицензии: бессрочная); – пакет математического моделирования Mathcad (Contract Number (SCN) 4A1913127. Срок действия лицензии: бессрочная); – система поиска заимствований в текстах «Антиплагиат ВУЗ» (Контракт № 0379400000323000002/1 от 27.02.2021 г. (срок действия от 01.03.2023 до 01.03.2024)); – Информационно-правовая система «Инофрмио» (Договор № НК 2846 от 18.01.2023 г.); – пакет визуального 3D-моделтрования Blender (Лицензия № GNU GPL v3. Срок действия лицензии: бессрочная); – векторный графический редактор Inkscape (Лицензия № GNU GPL v3. Срок действия лицензии: бессрочная);	369200, Карачаево-Черкесская Республика, г. Карачаевск, ул. Ленина, 29. Учебно-лабораторный корпус, ауд. 509

– программный комплекс для верстки Scribus (Лицензия № GNU GPL v3. Срок действия лицензии: бессрочная); – Autodesk AutoCAD (Лицензия № 5X6-30X999XX. Бессрочная образовательная (академическая) лицензия); – Autodesk 3DS Max (Лицензия № 5X5-93X928XX. Бессрочная образовательная (академическая) лицензия); Autodesk Revit (Лицензия № 5X6-03X109XX. Бессрочная образовательная (академическая) лицензия).	
Аудитория для самостоятельной работы обучающихся. Специализированная мебель: столы ученические, стулья, доска меловая. Учебно-наглядные пособия (в электронном виде). Технические средства обучения: ноутбуки в количестве 3 шт. с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета. *Лицензионное программное обеспечение:* – Microsoft Windows (Лицензия № 60290784), бессрочная – Microsoft Office (Лицензия № 60127446), бессрочная – ABBY Fine Reader (лицензия № FCRP-1100-1002-3937), бессрочная – Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная – Google G Suite for Education (IC: 01i1p5u8), бессрочная – Антивирус Касперского. Действует до 03.03.2025 г. (Договор № 56/2023 от 25 января 2023г.).	369200, Карачаево-Черкесская Республика, г. Карачаевск, ул. Ленина, 29. Учебно-лабораторный корпус, ауд. 507
Читальный зал, 80 мест, 10 компьютеров. *Специализированная мебель:* столы ученические, стулья. *Технические средства обучения:* Дисплей Брайля ALVA с программой экранного увеличителя MAGic Pro; стационарный видеоувеличитель CIear View с монитором; 2 компьютерных роллера USB&PS/2; клавиатура с накладкой (ДЦП); акустическая система свободного звукового поля Front Row to Go/$; персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета. *Лицензионное программное обеспечение:* – Microsoft Windows (Лицензия № 60290784), бессрочная – Microsoft Office (Лицензия № 60127446), бессрочная – ABBY Fine Reader (лицензия № FCRP-1100-1002-3937), бессрочная – Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная – Google G Suite for Education (IC: 01i1p5u8), бессрочная – Антивирус Касперского. Действует до 03.03.2025 г. (Договор № 56/2023 от 25 января 2023г.).	369200, Карачаево-Черкесская Республика, г. Карачаевск, ул. Ленина, 29. Учебно-лабораторный корпус, каб. 102 а.

10.3. 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

Для лиц с ОВЗ и/или с инвалидностью РПД разрабатывается на основании «Положения об организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в федеральном государственном бюджетном образовательном учреждении высшего образования «Карачаево-Черкесский государственный университет имени У. Д. Алиева».