

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Карачаево-Черкесский государственный университет имени У.Д. Алиева"

Педагогический факультет

Кафедра математики и методики ее преподавания



УТВЕРЖДАЮ

А.А. Узденова

«03» июля 2023г.

Рабочая программа дисциплины

**ОСНОВЫ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

(наименование дисциплины (модуля))

Направление подготовки

44.04.01 Педагогическое образование

(шифр, название направления)

Направленность (профиль) подготовки

***Информационные и коммуникационные
технологии в образовании***

Квалификация выпускника

магистр

Форма обучения

очная/заочная

Год начала подготовки-2023

(по учебному плану)

КАРАЧАЕВСК, 2023

Составитель: доц. Айбазова А.К.
Рецензенты: к.ф.-м.н., доц. Уртенев Н.С.

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 44.04.01 Педагогическое образование, утвержденного приказом Министерства образования и науки Российской Федерации от 22.02.2018 № 126, основной профессиональной образовательной программой высшего образования по направлению подготовки 44.04.01 Педагогическое образование, направленность (профиль): "Информационные и коммуникационные технологии в образовании"; локальными актами КЧГУ.

Рабочая программа рассмотрена и утверждена на заседании кафедры: *математики и методики ее преподавания* на 2023-2024 уч.год

Протокол № 12 от 3.07.2023г.

Зав. кафедрой



А.Х. Дзамыхов

СОДЕРЖАНИЕ

1. Наименование дисциплины (модуля).....	4
2. Место дисциплины (модуля) в структуре образовательной программы	4
3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.....	4
4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся.....	6
5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....	6
5.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах).....	6
5.2. Тематика лабораторных занятий	8
5.3. Примерная тематика курсовых работ.....	8
6. Образовательные технологии	9
7. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю).....	10
7.1. Описание шкал оценивания степени сформированности компетенций.....	10
7.2. Типовые контрольные задания или иные учебно-методические материалы, необходимые для оценивания степени сформированности компетенций в процессе освоения учебной дисциплины	11
7.2.1. Типовые темы к письменным работам, докладам и выступлениям:	11
7.2.2. Тестовые задания для проверки знаний студентов	12
7.2.3. Примерные вопросы к итоговой аттестации (экзамен)	17
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)	19
9. Методические указания для обучающихся по освоению учебной дисциплины (модуля).....	19
10. Требования к условиям реализации рабочей программы дисциплины (модуля)	20
10.1. Общесистемные требования	20
10.2. Материально-техническое и учебно-методическое обеспечение дисциплины	21
10.3. Необходимый комплект лицензионного программного обеспечения	21
10.4. Современные профессиональные базы данных и информационные справочные системы.....	21
11. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья.....	22
12. Лист регистрации изменений.....	23

1. Наименование дисциплины (модуля)

Основы информационной безопасности

Целью изучения дисциплины является ознакомить студентов с теоретическими основами информационной безопасности:

- изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.
- формирование знаний об объектах и задачах защиты компьютерных систем
- способах и средствах нарушения информационной безопасности, о принципах и подходах к решению задач защиты информации;
- формирование умений по применению современных технологий, выбора средств и инструментов защиты информации для построения современных защищенных информационных систем в соответствии с действующим законодательством.

2. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина (модуль) относится к Блоку 1 и реализуется в рамках базовой части Б1.

Дисциплина (модуль) изучается на 1_курсе (ах) в 2_семестре (ах).

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПВО	
Индекс	Б1.В.05
Требования к предварительной подготовке обучающегося:	
Дисциплина « Основы информационной безопасности » относится в дисциплинам по выбору общенаучного цикла (Б1.В.05). Список дисциплин, знание которых необходимо для изучения курса данной дисциплины: - « Инновационные процессы в образовании »; модуль « Методология и методы научного исследования » Результаты освоения дисциплины являются базовыми для осуществления различных видов научно-исследовательской работы, входящих в программу подготовки магистров.	
Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Результаты освоения дисциплины являются базовыми для осуществления различных видов научно-исследовательской работы, входящих в программу подготовки магистров. Изучение дисциплины необходимо для успешного освоения дисциплин профессионального цикла и практик, формирующих компетенции ПК-1	

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

В результате освоения ОПОП магистратуры обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

Код компетенций	Содержание компетенции в соответствии с ФГОС ВО/ ОПВО	Индикаторы достижения компетенций	Декомпозиция компетенций (результаты обучения) в соответствии с установленными индикаторами
ПК-1	ПК-1. Готовность реализовывать образовательные программы по	ПК-1.1. Знает: преподаваемый предмет; психолого-педагогические	Знать: вопросы административного и нормативно-правового обеспечения защиты

	<p>учебным предметам в соответствии с требованиями образовательных стандартов</p>	<p>основы и современные образовательные технологии; особенности организации образовательного процесса в соответствии с требованиями образовательных стандартов.</p> <p>ПК-1.2. Умеет: использовать педагогически обоснованные формы, методы и приемы организации деятельности обучающихся; применять современные образовательные технологии; создавать образовательную среду, обеспечивающую формирование у обучающихся образовательных результатов, предусмотренных ФГОС и(или) образовательными стандартами, установленными образовательной организацией, и(или) образовательной программой.</p> <p>ПК-1.3 Владеет навыками профессиональной деятельности по реализации программ учебных дисциплин в соответствии с требованиями образовательных стандартов.</p>	<p>информации основные системы защиты информации в России и в ведущих зарубежных странах;</p> <p>основные программно-аппаратные средства и методы защиты информации в компьютерных системах</p> <p>Уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения;</p> <p>Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.</p>
--	---	--	--

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 часов.

Объем дисциплины	Всего часов
	для очной формы обучения
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) * (всего)	
Аудиторная работа (всего):	16
лекции	
семинары, практические занятия	16
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 др.	
Контроль	
Самостоятельная работа обучающихся (всего)	92
Контроль самостоятельной работы	
Вид промежуточной аттестации обучающегося (зачет / экзамен)	экзамен-2,

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)			
			Аудиторные уч. занятия	Сам. работа	Планируемые результаты обучения	Формы текущего контроля
		всего				

	Раздел 1. Комплексный подход к обеспечению информационной безопасности						
1.	Введение в проблему информационной безопасности, ее актуальность.	8		2		6	ПК-1 Устный опрос
2.	Основные объекты информационных систем, подлежащих защите. Цели и задачи обеспечения информационной безопасности для различных объектов (правоохранительные органы, медучреждения, коммерческие организации и др.).	6				6	ПК-1 Доклад с презентацией
3.	Основные понятия информационной безопасности.	6				6	ПК-1 Блиц-опрос
4.	Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность.	8		2		6	ПК-1 Творческое задание
5.	Комплексный подход к защите информации. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический.	2		2			ПК-1 Блиц-опрос
6.	Требования к комплексным системам защиты информации.	6				6	ПК-1 Устный опрос
7.	Проанализировать профессионально-значимые источники информации с точки зрения основных аспектов:	8		2		6	ПК-1 Доклад с презентацией

	конфиденциальности, целостности и доступности.						
8.	Угрозы информационной безопасности в компьютерных системах	6			6	ПК-1	Фронтальный опрос
9.	Компьютерная система как объект защиты информации.	6			6	ПК-1	Доклад с презентацией
10.	Понятие угрозы информационной безопасности в компьютерных системах.	8		2	6	ПК-1	Блиц опрос
11.	Классификация и общий анализ угроз информационной безопасности в компьютерных системах.	6		2	4	ПК-1	Фронтальный опрос
12.	Случайные угрозы информационной безопасности.	4			4	ПК-1	Доклад с презентацией
13.	Преднамеренные угрозы информационной безопасности	6		2	4	ПК-1	Фронтальный опрос
14.	Законодательная и нормативно - правовая база РФ в области информатизации и защиты информации.	4			4	ПК-1	Тест
15.	Ответственность за нарушение законодательства в информационной сфере.	6		2	4	ПК-1	Фронтальный опрос
16.	Обзор зарубежного законодательства в области информационной безопасности.	4			4	ПК-1	Доклад с презентацией
17.	Итого	108		16	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 практических (семинарских, 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.

Практические (семинарские занятия относятся к интерактивным методам обучения и обладают значительными преимуществами по сравнению с традиционными методами обучения, главным недостатком которых является известная изначальная пассивность субъекта и объекта обучения.

Практические 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 нахождение истины или достижение лучшего взаимопонимания, Групповые обсуждения способствуют лучшему усвоению изучаемого материала.

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

Преподаватель может устанавливать определенные правила проведения группового обсуждения:

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

- ввести алгоритм выработки общего мнения (решения);

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

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

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

2.Публичная презентация проекта

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

3.Дискуссия

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

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

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

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

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

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

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

7.1. Описание шкал оценивания степени сформированности компетенций

Уровни сформированности компетенций	Индикаторы	Качественные критерии оценивание			
		2 балла	3 балла	4 балла	5 баллов
ПК-1					
Базовый	Знать: правила работы над совершенствованием принципов редактирования медиатекстов	Не знает особенности работы над совершенствованием принципов редактирования медиатекстов	В целом знает особенности работы над совершенствованием принципов редактирования медиатекстов	В целом знает особенности работы над совершенствованием принципов редактирования медиатекстов	
	Уметь: анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов	Не умеет анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов	В целом умеет анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов	Умеет анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов	
	Владеть: навыками редактирования медиатекстов	Не владеет навыками редактирования медиатекстов разных типов и	В целом владеет навыками редактирования медиатекстов	Владеет навыками редактирования медиатекстов разных типов и	

	разных типов и работать над их усовершенствованием	навыками работы над их усовершенствованием	разных типов и навыками работы над их усовершенствованием	навыками работы над их усовершенствованием	
Повышенный	Знать: правила работы над совершенствованием принципов редактирования медиатекстов				В полном объеме знает правила работы над совершенствованием принципов редактирования медиатекстов
	Уметь: анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов				В полном объеме умеет анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов
	Владеть: навыками редактирования медиатекстов разных типов и работать над их усовершенствованием				В полном объеме владеет навыками редактирования медиатекстов разных типов и навыками работы над их усовершенствованием

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:

«Основы информационной безопасности»

- 1 Угрозы информационной безопасности 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
- 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. Тестовые задания для проверки знаний студентов

Тестовые задания направлены на выявление подготовки студентов по курсу «Основы информационной безопасности». Каждый тест содержит три и более вариантов ответов, из которых необходимо выбрать верный. Максимально возможная отметка - 5.

(ПК-1) - Готовность реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

1. Под информационной безопасностью понимается...

А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность _____ .

4. Основные составляющие информационной безопасности _____ .

5. Доступность – это...

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

6. Целостность – это..

- А) целостность информации
- Б) непротиворечивость информации
- В) защищенность от разрушения

7. Конфиденциальность – это..

- А) защита от несанкционированного доступа к информации
- Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
- В) описание процедур

8. Для чего создаются информационные системы?

- А) получения определенных информационных услуг
- Б) обработки информации
- В) все ответы правильные

9. Целостность можно подразделить _____

10. Где применяются средства контроля динамической целостности?

- А) анализе потока финансовых сообщений
- Б) обработке данных
- В) при выявлении кражи, дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?

- А) сведения о технических каналах утечки информации являются закрытыми
- Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
- В) все ответы правильные

12. Угроза – это...

- А) потенциальная возможность определенным образом нарушить информационную безопасность
- Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
- В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это...

- А) попытка реализации угрозы
- Б) потенциальная возможность определенным образом нарушить информационную безопасность
- В) программы, предназначенные для поиска необходимых программ.

14. Источником угрозы является _____

15. Окно опасности – это...

- А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
- Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
- В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?

- А) должно стать известно о средствах использования пробелов в защите.

- Б) должны быть выпущены соответствующие заплаты.
- В) заплаты должны быть установлены в защищаемой И.С.

18. По каким компонентам классифицируется угрозы доступности:

- А) отказ пользователей
- Б) отказ поддерживающей инфраструктуры
- В) ошибка в программе

19. Основными источниками внутренних отказов являются:

- А) отступление от установленных правил эксплуатации
- Б) разрушение данных
- В) все ответы правильные

20. Основными источниками внутренних отказов являются:

- А) ошибки при конфигурировании системы
- Б) отказы программного или аппаратного обеспечения
- В) выход системы из штатного режима эксплуатации

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
- Б) обрабатывать большой объем программной информации
- В) нет правильного ответа

22. Скажите существующие грани вредоносного П.О. _____

23. По механизму распространения П.О. различают _____

24. Вирус – это...

- А) код обладающий способностью к распространению путем внедрения в другие программы
- Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
- В) небольшая программа для выполнения определенной задачи

25. Черви – это...

- А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
- Б) код обладающий способностью к распространению путем внедрения в другие программы
- В) программа действий над объектом или его свойствами

26. Конфиденциальную информацию на что можно разделить _____

27. Природа происхождения угроз _____

28. Предпосылки появления угроз _____

29. К какому виду угроз относится присвоение чужого права?

- А) нарушение права собственности
- Б) нарушение содержания
- В) внешняя среда

30. Отказ, ошибки, сбой в компьютере _____

31. Отказ - это...

- А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
- Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
- В) структура, определяющая последовательность выполнения и взаимосвязи процессов

32. Ошибка – это...

- А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
- Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
- В) негативное воздействие на программу

33. Сбой – это...

- А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
- Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
- В) объект-метод

34. Побочное влияние – это...

- А) негативное воздействие на систему в целом или отдельные элементы
- Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
- В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

35. СЗИ (система защиты информации) делится:

- А) ресурсы автоматизированных систем
- Б) организационно-правовое обеспечение
- В) человеческий компонент

36. Что относится к человеческому компоненту СЗИ?

- А) системные порты
- Б) администрация
- В) программное обеспечение

37. Что относится к ресурсам А.С. СЗИ?

- А) лингвистическое обеспечение
- Б) техническое обеспечение
- В) все ответы правильные

38. По уровню обеспеченной защиты все системы делят:

- А) сильной защиты
- Б) особой защиты
- В) слабой защиты

39. По активности реагирования СЗИ системы делят:

- А) пассивные
- Б) активные
- В) полупассивные

40. Правовое обеспечение безопасности информации – это...

- А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
- Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
- В) нет правильного ответа

41. Правовое обеспечение безопасности информации делится:

- А) международно-правовые нормы
- Б) национально-правовые нормы
- В) все ответы правильные

42. Информацию с ограниченным доступом делят:

- А) государственную тайну
- Б) конфиденциальную информацию
- В) достоверную информацию

43. Что относится к государственной тайне?

- А) сведения, защищаемые государством в области военной, экономической ... деятельности
- Б) документированная информация
- В) нет правильного ответа

44. Вредоносная программа - это...

- А) программа, специально разработанная для нарушения нормального функционирования систем
- Б) упорядочение абстракций, расположение их по уровням
- В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

45. Основопологающие документы для обеспечения безопасности внутри организации:

- А) трудовой договор сотрудников
- Б) должностные обязанности руководителей
- В) коллективный договор

46. К организационно - административному обеспечению информации относится:

- А) взаимоотношения исполнителей
- Б) подбор персонала
- В) регламентация производственной деятельности

47. Какие средства используются на инженерных и технических мероприятиях в защите информации _____

49. Программные средства – это...

- А) специальные программы и системы защиты информации в информационных системах различного назначения
- Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
- В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

50. Криптографические средства – это...

- А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах

с использованием методов шифрования

Б) специальные программы и системы защиты информации в информационных системах различного назначения

В) механизм, позволяющий получить новый класс на основе существующего

7.2.3. Примерные вопросы к итоговой аттестации (экзамен)

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. Какими способами снизить угрозу sniffing пакетов?
11. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?
25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27. В чем заключается контроль участников взаимодействия?
28. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?
- 12
30. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
31. Какой процесс называется аутентификацией пользователя?
32. Какие схемы аутентификации вы знаете?

33. Что такое смарт-карты?
34. Какие требования предъявляются к современным криптографическим системам защиты информации?
35. Что такое симметричная криптосистема?
36. Какие виды симметричных криптосистем существуют?
37. Что такое асимметричная криптосистема?
38. Что понимается под односторонней функцией?
39. Как классифицируются криптографические алгоритмы по стойкости?
40. В чем заключается анализ надежности криптосистем?
41. Что такое дифференциальный криптоанализ?
42. В чем сущность криптоанализа со связанными ключами?
43. В чем сущность линейного криптоанализа?
44. Какие атаки изнутри вы знаете?
45. Какая программа называется логической бомбой?
46. Какими способами можно проверить систему безопасности?
47. Что является основными характеристиками технических средств защиты информации?
48. Какие требования предъявляются к автоматизированным системам защиты третьей группы?
49. Какие требования предъявляются к автоматизированным системам защиты второй группы?
50. Какие требования предъявляются к автоматизированным системам защиты первой группы?
51. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52. Какие требования предъявляются к межсетевым экранам?
53. Какие имеются показатели защищенности межсетевых экранов?
54. Какие атаки системы снаружи вы знаете?
55. Какая программа называется вирусом?
56. Какая атака называется атакой отказа в обслуживании?
57. Какие виды вирусов вы знаете?
58. Какие вирусы называются паразитическими?
59. Как распространяются вирусы?
60. Какие методы обнаружения вирусов вы знаете?
61. Какая программа называется монитором обращения?
62. Что представляет собой домен?
63. Как осуществляется защита при помощи ACL -списков?
64. Какой список называется перечнем возможностей?
65. Какие способы защиты перечней возможностей вы знаете?

Критерии оценки устного ответа на вопросы по дисциплине

«Введение в профессию»:

✓ 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.

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

8.1. Основная литература:

1. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. – Москва.- РИОР ИНФА-М. 2022- 202, <https://znanium.com/read?id=393455>
2. Зенков А.В. Основы информационной безопасности: учебное пособие/ А.В. Зенков, Москва, - Вологда, ИНФА-Инженерия, -2022, - 104, ил.,таб. - <https://znanium.com/read?id=417201>
3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф.- Саратов: Профобразование, 2017.— 544 с.— Режим доступа: URL <https://znanium.com/catalog/document?id=435364>

8.2. Дополнительная литература:

1. Федотова, Е. Л. Информационные технологии и системы : учебное пособие / Е. Л. Федотова. - Москва : ФОРУМ : ИНФРА-М, 2020. - 352 с. - URL: <https://znanium.com/read?id=421073> - Режим доступа: по подписке. - Текст: электронный.
2. Иванов, М. И. Информатика: основные понятия и тесты : учебное пособие / М. И. Иванов, Ю. Г. Уткин. - Москва : МГАВТ, 2007. - 192 с. - URL: <https://znanium.com/catalog/product/401201>- Режим доступа: по подписке. - Текст: электронный.

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 удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом
Контрольная работа/ индивидуальные	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и

задания	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
2023 / 2024 учебный год	Договор №915 ЭБС ООО «Знаниум» от 12.05.2023г. Действует до 15.05.2024г.	от 12.05.2023г. до 15.05.2024г.
	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

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

369200, Карачаево-Черкесская Республика, г. Карачаевск, ул. Ленина, 29. Учебный корпус №4, ауд. 423.

Учебная аудитория для проведения занятий лекционного и практического типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации

Специализированная мебель:

столы ученические, стулья, шкафы.

Технические средства обучения:

Персональные компьютеры с подключением к информационнотелекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета - 7 шт

Периодические издания по педагогике.

Лицензионное программное обеспечение:

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

1.Мультимедийный кабинет: интерактивная доска с проектором, компьютеры с доступом в Интернет (41 аудитория, 3 этаж 1 учебного корпуса)

2. Интерактивный монитор с компьютером; плазменный телевизор, подключенный к компьютеру (49 аудитория, 3 этаж 1 учебного корпуса)

3.Компьютерный класс: 10 компьютеров, подключенных к сети Интернет, интерактивный монитор с компьютером, цифровая видеокамера, цифровой фотоаппарат, 4 цифровых диктофона, телевизионная система со спутниковой антенной и DVD- плеером (42 аудитория, 3 этаж 1 учебного корпуса)

4.Общеуниверситетский компьютерный центр обучения и тестирования: 24 компьютеризированных мест (210 аудитория, 2 этаж 4 учебного корпуса)

5.Студенческий читальный зал на 65 мест (18 компьютеризированы с подключением к сети Интернет);

6.Читальный зал периодики на 25 мест;

7.Научный зал на 25 мест, 10 из которых оборудованы компьютерами.

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

10.3. Необходимый комплект лицензионного программного обеспечения

- MicrosoftWindows (Лицензия № 60290784), бессрочная
- MicrosoftOffice (Лицензия № 60127446), бессрочная
- ABBY FineReader (лицензия № FCRP-1100-1002-3937), бессрочная
- CalculateLinux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная
- Google G Suite for Education (IC: 01i1p5u8), бессрочная
- Kaspersky Endpoint Security (Лицензия № 280E-210210-093403-420-2061), с25.01.2023по 03.03.2025г.

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.ur?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») - <https://www.big-big.ru/besplatno/window.edu.ru.html>.

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 позиция 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 Board», «Toshiba»;
- экраны проекционные на штативе 280*120;
- мультимедиа-проекторы Epson, Benq, Mitsubishi, Aser;

2. Презентационное оборудование:

- радиосистемы AKG, Shure, Quik;
- видеоконфликты 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

В рабочей программе внесены следующие изменения:

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