ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 1060A5DD076C1D70B8BBAD48EDF7B4FB
Владелец: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА"
Действителен: с 18.04.2024 до 12.07.2025

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯРОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждениевысшего образования
"Карачаево-Черкесский государственный университет имени У.Д. Алиева"

ФАКУЛЬТЕТ ФИЗИЧЕСКОЙ КУЛЬТУРЫ

КАФЕДРА ТЕОРЕТИЧЕСКИХ ОСНОВ ФИЗИЧЕСКОЙ КУЛЬТУРЫ И ТУРИЗМА

УТВЕРЖДАЮ
И. о. проректора по УР
М. Х. Чанкаев
«29» мая 2024 г., протокол № 8

Рабочая программа дисциплины

Информационная безопасность

(наименование дисциплины (модуля)

Направление подготовки

44.03.05 – Педагогическое образование (с двумя профилями подготовки)

(шифр, название направления)

Направленность (профиль) подготовки

Физическая культура, безопасность жизнедеятельности

Квалификация выпускника

бакалавр

Форма обучения

Очная/заочная

Год начала подготовки - 2021

(по учебному плану)

Карачаевск, 2024

Составитель: ст. преподаватель каф. ИВМ Чомаева З.У.

Рабочая программа дисциплины составлена в соответствии с требованиями федерального государственного образовательного стандартавысшего образования по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) профиль «Физическая культура, безопасность жизнедеятельности» № 125 от 22.02.2018 г., образовательной программой высшего образования, локальными актами КЧГУ.

Рабочая программа рассмотрена и утверждена на заседании кафедры

информатики и вычислительной математики на 2024-2025 уч. год

Протокол № 9 от 07.05.2024 года

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ 3
Для достижения цели ставятся задачи: 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 преподава- 6
5. Содержание дисциплины (модуля), структурированное по темам (разделам) суказанием отведенного на них количества академических часов и видов учебных за- 6
5.1. Разделы дисциплины и трудоемкость по видам учебных занятий(в академических часах) 6
5.2. Тематика лабораторных занятий 9
5.3. Примерная тематика курсовых работ 9
6. Образовательные технологии 9
Развитие у обучающихся навыков командной работы, межличностной комму- никации, принятия решений и лидерских качеств при проведении учебных занятий 9
7. Фонд оценочных средств для проведения текущего контроля и промежуточной ат- тестации обучающихся по дисциплине (модулю) 10
7.1. Описание шкал оценивания степени сформированности компетенций 10
7.2. Типовые контрольные задания или иные учебно-методические материалы, необ- ходимые для оценивания степени сформированности компетенций в процессе освое- ния учебной дисциплины 12
7.2.1.Типовые темы к письменным работам, докладам и выступлениям: 12
Критерии оценки доклада, сообщения, реферата: 13
7.2.2.Примерные вопросы к итоговой аттестации (экзамен) 13
Критерии оценки устного ответа на вопросы по дисциплине 14
7.2.3.Тестовые задания для проверки знаний студентов 15
Методические материалы, определяющие процедуры оценивания знаний 19
Критерии оценки тестового материала по дисциплине 19
7.2.4.Бально-рейтинговая система оценки знаний бакалавров 19
Таблица перевода балльно-рейтинговых показателей в отметки традиционнойсистемы оценивания 20
8. Перечень основной и дополнительной учебной литературы, необходимой для осво-ения дисциплины. Информационное обеспечение образовательного процесса 21
8.1. Основная литература: 21
8.2. Дополнительная литература 21
Ресурсы ЭБС 22
9. Требования к условиям реализации рабочей программы дисциплины (модуля 22
9.1. Общесистемные требования 22
9.2. Материально-техническое и учебно-методическое обеспечение дисциплины 23
9.4. Современные профессиональные базы данных и информационные справочные системы 23
10. Особенности организации образовательного процесса для лиц с ограниченными возможностями здоровья 23
11. Лист регистрации изменений 23

1. Наименование дисциплины(модуля)

Информационная безопасность

Целью изучения дисциплины является: формирование у бакалавров профессиональных и универсальных компетенций путем изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Для достижения цели ставятся задачи:

- получить представление о правилах защиты информации;
- изучить методы и средства обеспечения защиты информации
- изучить необходимый понятийный аппарат дисциплины;
- сформировать умение проводить анализ угроз безопасности;
- сформировать навыки использования методов и средств защиты информации Цели и задачи дисциплины определены в соответствии с требованиями Федерально-

го государственного образовательного стандарта высшего образования по направлению подготовки «44.03.05 Педагогическое образование (с двумя профилями подготовки), профиль – Физическая культура; безопасность жизнедеятельности» (квалификация – «ба- калавр»).

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность» (Б1.О.21) относится к

обязательной частиДисциплина (модуль) изучается на 5 курсе в семестре А.

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО	
Индекс	Б1.О.21
Требования к предварительной подготовке обучающегося:	
Для освоения учебной дисциплины «Информационная безопасность» студент должен иметь базовые знания, полученные при изучении школьной программы математики, основ информатики и компьютерных технологий.	
Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Курс «Информационная безопасность» является основой для последующего успешного прохождения всех видов практик и для успешного прохождения итоговой государственной аттестации.	

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

Процесс изучения дисциплины «Информационная безопасность» н

аправлен наформирование следующих компетенций обучающегося:

Код компетенций	Содержание компетенции в соответствии с ФГОС ВО/ ПООП/ ООП	Индикаторы достижения компетенций	Декомпозиция компетенций (результаты обучения) в соответствии с установленными индикаторами

ОПК-9	ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-9.1. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности. ОПК-9.2. Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности.	**Знать**: базовые понятия информатики и ИКТ, используемые в области защиты информации и обеспечения информационной безопасности; современное состояние и тенденции развития методов защиты информации; организационно-правовое обеспечение информационной безопасности; технологии эффективной защиты информации и информационной безопасности. **Уметь**: Классифицировать угрозы информационной безопасности объекта. **Владеть**: Основными методами защиты информации; практическими навыками организации защиты информации и обеспечения информационной безопасности.
УК-1	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Демонстрирует знание особенностей системного и критического мышления, аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение. УК-1.2. Применяет логические формы и процедуры, способен к рефлексии по поводу собственной и чужой мыслительной деятельности. УК-1.3. Анализирует источники информации с целью выявления их противоречий и поиска достоверных суждений.	**Знать** – принципы анализа информации, основные справочные системы, профессиональные базы данных, требования информационной безопасности **Уметь**: использовать стандартные пакеты (библиотеки) языка для решения практических задач; решать исследовательские и проектные задачи с использованием компьютеров. **Владеть**: методами построения современных проблемно-ориентированных прикладных программных средств; методами и средствами разработки и оформления

УК-2	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Определяет совокупность взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм. УК-2.2. Оценивает вероятные риски и ограничения, определяет ожидаемые результаты решения поставленных задач. УК-2.3. Использует инструменты и техники цифрового моделирования для реализации образовательных процессов.	**Знать**: основные принципы аппаратно-программной защиты информации. **Уметь**: реагировать на различные угрозы информационной безопасности. **Владеть** навыками применения и настройки антивирусных систем и систем распознавания угроз и атак

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 академи-ческих часа.

Объѐм дисциплины	Всего часов	Всего часов
	для очной формы обучения	для заочной формы обучения
Общая трудоемкость дисциплины	108	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)	48	8
Аудиторная работа (всего):	48	48
в том числе:		
лекции	24	2
семинары, практические занятия	24	6
практикумы	-	-
лабораторные работы		
Внеаудиторная работа:		
консультация перед зачетом		
Внеаудиторная работа также включает индивидуальную работу обучающихся с преподава- телем, групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем), творческую работу (эссе), рефераты, контрольные работы и др.		
Самостоятельная работа обучающихся (всего)	60	92
Контроль самостоятельной работы		8
Вид промежуточной аттестации обучающегося (зачет / экзамен)	экзамен	экзамен

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

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

Для очной формы обучения

№ п/п	Раздел, тема дисциплины	Общая трудоемкость (в часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость(в часах)					
		всего	Аудиторные уч. занятия			Сам. работа	Планируемые результаты обучения	Формы текущего контроля
			Лек	Пр	Лаб			
	Раздел 1.							
1.	Тема: Проблемы обеспечения информационной безопасности	10	2	2		6	ОПК-9 УК-1 УК-2	Устный опрос
2.	Тема: Составляющие информационной безопасности	10	2	2		6	ОПК-9 УК-1 УК-2	Доклад с презентацией
3.	Тема: Основы шифрования данных.	8	2	2		4	ОПК-9 УК-1 УК-2	Творческое задание
4.	Тема: История криптографии	8	2	2		4	ОПК-9 УК-1 УК-2	Блиц-опрос
5.	Тема: Угрозы информационной безопасности	8	2	2		4	ОПК-9 УК-1 УК-2	Тест
6.	Тема: Методы реализации угроз информационной безопасности	10	2	2		6	ОПК-9 УК-1 УК-2	Реферат
7.	Тема: Нормативно-правовые основы информационной безопасности в РФ	8	2	2		4	ОПК-9 УК-1 УК-2	Тест
8.	Тема: Основные положения важнейших законодательных актов РФ в области информационной безопасности и информации	10	2	2		6	ОПК-9 УК-1 УК-2	Реферат
9.	Тема: Информационная война */ср/*	10	2	2		6	ОПК-9 УК-1 УК-2	Творческое задание
10.	Тема: Обеспечение информационной безопасности операционных систем	8	2	2		4	ОПК-9 УК-1 УК-2	Устный опрос
11.	Тема: Механизмы обеспечения информационной безопасности в информационных системах.	8	2	2		4	ОПК-9 УК-1 УК-2	Доклад с презентацией
12.	Тема: Методы и средства защиты информации в сети Интернет	10	2	2		6	ОПК-9 УК-1 УК-2	Творческое задание
	Итого;	**108**	**24**	**24**		**60**		

Для заочной формы обучения

№ п/п	Раздел, тема дисциплины	Общая трудоемкость (в часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость(в часах)					
		всего	Аудиторные уч. занятия			Сам. работа	Планируемые результаты обучения	Формы текущего контроля
			Лек	Пр	Лаб			
	Раздел 1.							
	Тема: Проблемы обеспечения информационной безопасности	8	2			6	ОПК-9 УК-1 УК-2	Устный опрос
2.	Тема: Составляющие информационной безопасности	10		2		8	ОПК-9 УК-1 УК-2	Доклад с презентацией
3.	Тема: Основы шифрования данных.	8				8	ОПК-9 УК-1 УК-2	Творческое задание
4.	Тема: История криптографии	10		2		8	ОПК-9 УК-1 УК-2	Блиц-опрос
5.	Тема: Угрозы информационной безопасности	8				8	ОПК-9 УК-1 УК-2	Тест
6.	Тема: Методы реализации угроз информационной безопасности	8				8	ОПК-9 УК-1 УК-2	Реферат
7.	Тема: Нормативно-правовые основы информационной безопасности в РФ	8				8	ОПК-9 УК-1 УК-2	Тест
8.	Тема: Основные положения важнейших законодательных актов РФ в области информационной безопасности и информации	12		2		10	ОПК-9 УК-1 УК-2	Реферат
9.	Тема: Информационная война	6				6	ОПК-9 УК-1 УК-2	Творческое задание
10.	Тема: Обеспечение информационной безопасности операционных систем	8				8	ОПК-9 УК-1 УК-2	Устный опрос
11.	Тема: Механизмы обеспечения информационной безопасности в информационных системах	6				6	ОПК-9 УК-1 УК-2	Доклад с презентацией
12.	Тема: Методы и средства защиты информации в сети Интернет	8				8	ОПК-9 УК-1 УК-2	Творческое задание
	Контроль	**8**						

	Итого;	**108**	**2**	**6**		**92**		

5.2. Тематика лабораторных занятий

Учебным планом не предусмотрено

5.3. Примерная тематика курсовых работ

Учебным планом не предусмотрено

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 про- цессе 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 комму- никации, 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 ин- формацию, 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.

Обсуждение в группах

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

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

Преподаватель может устанавливать определенные правила проведения группового обсуждения:

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

-ввести алгоритм выработки общего мнения (решения);

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

На втором этапе группового обсуждения вырабатывается групповое решение сов- местно с преподавателем (арбитром).

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

Публичная презентация проекта

Презентация – самый эффективный способ донесения важной информации как в раз- говоре «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.

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 ат-тестации обучающихся по дисциплине (модулю)

7.1. Описание шкал оценивания степени сформированности компетенций

Уровни сформированности компетенций	Индикаторы	Качественные критерии оценивание			
		2 балла	3 балла	4 балла	5 баллов
УК-1; УК-2					
Базовый	**Знать:** совокупность политических, экономических факторов, право-	Не знает полити- ческих, экономи- ческих факторов, правовых и эти- ческих норм, ре-	В целом знает политические, экономические факторы, право- вые и этические	Знает совокуп- ность политиче- ских, экономиче- ских факторов, правовых и эти-	

	вых и этических норм, регулирующих развитие разных медиакоммуникационных систем на глобальном, национальном и региональном уровнях	гулирующих развитие разных медиакоммуникационных систем на глобальном, национальном и региональном уровнях	нормы, регулирующие развитие разных медиакоммуникационных систем на глобальном, национальном и региональном уровнях	ческих норм, регулирующих развитие разных медиакоммуникационных систем на глобальном, национальном и региональном уровнях	
	Уметь: реализовывать свои профессиональные журналистские действия с учетом механизмов функционирования конкретной медиакоммуникационной системы	Не умеетреализовывать свои профессиональные журналистские действия с учетом механизмов функционирования конкретной медиакоммуникационной системы	В целом умеет реализовывать свои профессиональные журналистские действия с учетом механизмов функционирования конкретной медиакоммуникационной системы	Умеетреализовывать свои профессиональные журналистские действия с учетом механизмов функционирования конкретной медиакоммуникационной системы	
	Владеть: навыками работы над созданием медиатекстов на основе экономических меха-	Не владеет навыками работы над созданием медиатекстов на основе экономических механиз-	В целом владеет навыками работы над созданием медиатекстов на основе экономических механиз-	Владеет навыками работы над созданием медиатекстов на основе экономических механиз-	
	низмов функционирования СМИ и соблюдения правовых и этических норм регулирования профессиональной деятельности	мов функционирования СМИ и соблюдения правовых и этических норм регулирования профессиональной деятельности	мов функционирования СМИ и соблюдения правовых и этических норм регулирования профессиональной деятельности	мов функционирования СМИ и соблюдения правовых и этических норм регулирования профессиональной деятельности	
Повышенный	**Знать:** совокупность политических, экономических факторов, правовых и этических норм, регулирующих развитие разных медиакоммуникационных систем на глобальном, национальном и региональном уровнях				В полном объеме знает совокупность политических, экономических факторов, правовых и этических норм, регулирующих развитие разных медиакоммуникационных систем на глобальном, национальном и региональном уровнях
	Уметь: реализовывать свои профессиональные журналистские действия с учетом механизмов функционирования конкретной медиакоммуни-				Умеет в полном объеме реализовывать свои профессиональные журналистские действия с учетом механизмов функционирования конкретной медиакоммуника-

	кационной системы				ционной системы
	Владеть: навыками работы над созданием медиатекстов на основе экономических механизмов функционирования СМИ и соблюдения правовых и этических норм регулирования профессиональной деятельности				В полном объеме владеет навыками работы над созданием медиатекстов на основе экономических механизмов функционирования СМИ и соблюдения правовых и этических норм регулирования профессиональной деятельности
ОПК-9					
Базовый	**Знать:** особенностиработы над сбором, проверкой и анализом информации	Не знает особенностей работы над сбором, проверкой и анализом информации	В целом знает особенностиработы над сбором, проверкой и анализом информации	Знает особенностиработы над сбором, проверкой и анализом информации	
	Уметь: выбирать актуальные темы и	Не умеет выбирать актуальные темы и проблемы	В целом умеет выбирать актуальные темы и	Умеет выбирать актуальные темы и проблемы для	
	проблемы для публикации	для публикации	проблемы для публикации	публикации	
	Владеть: навыками работы над созданием текстов на актуальные темы	Не владеет навыками работы над созданием текстов на актуальные темы	В целом владеет навыками работы над созданием текстов на актуальные темы	Владеет навыками работы над созданием текстов на актуальные темы	
Повышенный	**Знать:** особенностиработы над сбором, проверкой и анализом информации				В полном объеме владеет навыками работы над сбором, проверкой и анализом информации
	Уметь: выбирать актуальные темы и проблемы для публикации				В полном объеме владеет навыками работы, выбирает актуальные темы и проблемы для публикации
	Владеть: навыками работы над созданием текстов на актуальные темы				В полном объеме владеет навыками работы над созданием текстов на актуальные темы

7.2. Типовые контрольные задания или иные учебно-методические материалы, необ- ходимые для оценивания степени сформированности компетенций в процессе освое- ния учебной дисциплины

7.2.1. Типовые темы к письменным работам, докладам и выступлениям:

1. Составляющие информационной безопасности.
2. История криптографии.

3. Методы реализации угроз информационной безопасности.
4. Законодательные акты РФ в области информационной безопасности и защи-тыинформации.
5. Информационная война.
6. Основные требования к шифрам.
7. Алгоритмы хэширования.
8. Факторы, определяющие качество антивирусных программ.
9. Основные функции подсистемы защиты операционной системы.
10. Технологии межсетевых экранов.

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 былиправильными.

7.2.2. Примерные вопросы к итоговой аттестации (экзамен)

1. Понятия «информационная безопасность» и «защита информации»
2. Уровни формирования режима информационной безопасности
3. Административный уровень обеспечения информационной безопасности
4. Классификация угроз информационной безопасности
5. Анализ угроз информационной безопасности (угрозы нарушения доступности, целостности и конфиденциальности информации)
6. Модель угроз, модель нарушителя
7. Правовые основы информационной безопасности общества
8. Стандарты информационной безопасности
9. Виды конфиденциальной информации
10. Защита интеллектуальной собственности средствами патентного и авторского права
11. Назначение электронной цифровой подписи
12. Процедуры цифровой подписи

13. Функция хэширования
14. Вредоносные программы как угроза информационной безопасности
15. Методы обнаружения вредоносных программ
16. Антивирусные программы
17. Защита от несанкционированного доступа в компьютерных системах
18. Идентификация и аутентификация пользователей и программ
19. Методы аутентификации, использующие пароли и PIN-коды
20. Угрозы безопасности операционной системы
21. Понятие защищенной операционной системы
22. Архитектура подсистемы защиты операционной системы
23. Разграничение доступа к объектам операционной системы
24. Инженерная защиты объекта информатизации
25. Техническая охрана объекта информатизации

Реализация гуманитарного подхода в процессе использования информационно-коммуникационных технологий в учебном процессе. 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 по-сле наводящих вопросов, или не на все вопросы.

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

- не достаточно 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 правиль-ными.

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 былиправильными.

Критерии оценки устного ответа на вопросы по дисциплине «Введение в профессию»:

✓ 5 баллов - если ответ показывает глубокое и систематическое знание всего про- граммного 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 убе- дительное 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; отсутствиелогической связи в ответе.

7.2.3. Тестовые задания для проверки знаний студентов

1. (ОПК-9)

Защита информации – это..

комплекс мероприятий, направленных на обеспечение информа-ционной безопасности

процесс сбора, накопления, обработки, хранения, распределения ипоиска информации

процесс разработки структуры базы данных в соответствии с требованиями пользователей

небольшая программа для выполнения определенной задачи

2. (ОПК-9)

Какой термин определяет защищенность информации, ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам ин- формационных отношений — производителям, владельцам и пользователям информации и поддерживающей инфраструктуре?

стратегическая безопасность

информационная безопасность

экономическая безопасность

корпоративная безопасность

3. (ОПК-9)

Гарантия получения требуемой информации или информационной услугипользов

целостностью

доступностью

конфиденциальностью

4. (ОПК-9)

Гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена называется …

целостностью

доступностью

конфиденциальностью

5. (ОПК-9)

Какой аспект информационной безопасности отражает актуальность и непротиворечи

вость информации, её защищенность от разрушения и несанкционированного изменения?
целостность
конфиденциальность
доступность

6. (ОПК-9)
Если злоумышленник подменил исходное сообщение, передаваемое по сети Интернет,какое свойство информации он нарушил?
целостность
конфиденциальность
доступность
7. (ОПК-9)
Если в результате DoS-атаки злоумышленников сайт перестал работать, какой аспект информационной безопасности был нарушен?
целостность
конфиденциальность
доступность
8. (ОПК-9)
Как называется совокупность условий и факторов, создающих потенциальную илиреально существующую опасность нарушения безопасности информации?
атака
угроза
уязвимость
слабое место системы

9. (УК-1)
Кто такой инсайдер?
сотрудник, являющийся источником утечки информации
любой источник утечки информации
программа-вирус являющаяся источником утечки информации

10. (УК-1)
Как называется модель, описывающая вероятный облик злоумышленника, т. е. его квалификацию, имеющиеся средства для реализации тех или иных атак, обычное время действия и т. п?
модель угрозы
модель уязвимости
модель нарушителя
модель безопасности

11. (УК-1)
Какой уровень защиты информации представляет собой комплекс мер, применяемых руководством организации?
законодательный
процедурный
программно-технический
административный
12. (УК-1)
К какому уровню обеспечения ИБ относится «Доктрина информационной безопасности Российской Федерации»?
законодательный

административный
процедурный
научно-технический

13. (УК-1)
В каком законе РФ прописано индивидуальные право каждого гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом?
закон «О персональных данных»
закон «Об электронной подписи»
Конституция РФ
Доктрина информационной безопасности
14. (УК-1)
К какой категории охраняемой информации относится врачебная тайна?
государственная тайна
служебная тайна
профессиональная тайна
объекты авторского права

15. (УК-1)
Какой из законов РФ назначает уголовную ответственность за неправомерный доступ ккомпьютерной информации?
Уголовный кодекс РФ
Гражданский кодекс РФ
Конституция РФ
Доктрина информационной безопасности

16. (УК-1)
Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?
асимметричный
симметричный
правильного ответа нет

17. (УК-1)
Процесс нахождения открытого сообщения соответственно заданному закрытому прине-известном криптографическом преобразовании называется:
шифрование
дешифровка
расшифровка
18. (УК-1)
В каких основных форматах существует симметричный алгоритм?
блока и строки;
потока и блока;
потока и данных

19. (УК-1)
Открытым текстом в криптографии называют:
расшифрованный текст
любое послание
исходное послание
20. (УК-1)
Какой ключ известен только приемнику?

открытый
закрытый21. (УК-2)
Наука, занимающаяся защитой информации, путем преобразования этой информации это:
криптография
криптология
криптоанализ

22. (УК-2)
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
23. (УК-2)
Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:
шифр функциональных преобразований
шифр замен
шифр перестановок

24. (УК-2)
Шифрование-
это:
процесс создания алгоритмов шифрования
процесс сжатия информации
процесс криптографического преобразования информации к ви-ду, когдаее смысл полностью теряется

25. (УК-2)
Стойкость ключа характеризуется
длинной
непредсказуемостью
все варианты правильные
правильного варианта нет

26. (УК-2)
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

27. (УК-2)
Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый?
нет
да
в редких случаях

28. (УК-2)
Аутентификацией называют:
процесс регистрации в системе

способ защиты системы
процесс распознавания и проверки подлинности заявлений осебе пользователей и процессов

29. (УК-2)
Атака – это…
попытка реализации угрозы
потенциальная возможность определенным образомнарушить информационную безопасность
программы, предназначенные для поиска необходимых программ

30. (УК-2)
Наличие межсетевого экрана необходимо при?
использовании автономного автоматизированного рабочего места
использовании сетей общего пользования
использовании изолированной локальной сети

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
«Введение в профессию»:

✓ 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 объѐме; имеются незначительные методические недочѐты 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 пре- подаватель 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 од- ного 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 бал- лов, 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 де- каната.

«Корректировка баллов за пропуски» - графа заполняется делопроизводителем дека-
ната.

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

Таблица перевода балльно-рейтинговых показателей в отметки традиционнойсистемы оценивания

Соотношение часов лекцион- ных и практи- ческих 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 по- казателей тра- диционной отметке	1,5	1,1	1,1	1,1	1,1	1,1	1,1	1,1	1,1	«зачтено»
	1	1	1	1	1	1	1	1	1	«удовлетворительно»
	2	1,75	1,65	1,6	1,5	1,4	1,35	1,25	-	«хорошо»
	3	2,5	2,3	2,2	2	1,8	1,7	1,5	-	«отлично»

Необходимое количество баллов для выставления отметок («зачтено», «удовлетворительно», «хорошо», «отлично») определяется произведением реально проведенных

аудиторных часов (n) за отчетный период на коэффициент соответствия в зависимости от соотношения часов лекционных и практических занятий согласно приведенной таблице.

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

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

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

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

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

8.1. Основная литература:

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее обра- зование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013711 (да- та обращения: 12.03.2021). – Режим доступа: по подписке.
2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах :учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : элек- тронный. - URL: https://znanium.com/catalog/product/1093695 (дата обращения: 12.03.2021). – Режим доступа: по подписке.
3. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - Москва : ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. (Высшее образование: Бакалавриат; Магистратура). ISBN 978-5-369-01378-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/474838 (дата обращения: 12.03.2021). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Баранова, Е. К. Основы информатики и защиты информации : учебное по- собие / Е. К. Баранова. - Москва : РИОР : ИНФРА-М, 2013. - 183 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01169-0 (РИОР), ISBN 978-5-16- 006484-0 (ИНФРА-М). - Текст : электронный. - URL: https://znanium.com/catalog/product/415501 (дата обращения: 06.03.2021). – Режим доступа: по подписке.
2. Криптографическая защита информации : учебное пособие / С. О. Крама- ров, О. Ю. Митясова, С. В. Соколов *и др.+ ; под ред. С. О. Крамарова. — Москва : РИОР : ИНФРА-М, 2021. — 321 с.

— (Высшее образование). - ISBN 978-5-369-01716-6. - Текст : электронный. - URL:https://znanium.com/catalog/product/1153156 (дата обращения: 12.03.2021).
– Режим доступа: по подписке.

Ресурсы ЭБС.

http://www.edu.ru/ - Федеральный портал «Российское образование»
http://www.school.edu.ru - Российский общеобразовательный портал
http://window.edu.ru-
Единое окно доступа к образовательным ресурсам
http://school-collection.edu.ru- Единая коллекция цифровых образовательныхресурсов
http://fcior.edu.ru/ - Федеральный центр информационно-образовательных ресурсов http://www.fipi.ru/- Федеральный институт педагогических измерений http://www.ege.edu.ru/ - Официальный портал Единого Государственного Экзамена http://36edu.ru/default.aspx -
Департамент образования, науки и молодежной политики Московской области

9. *Требования к условиям реализации рабочей программы дисциплины (модуля*)

9.1. Общесистемные требования

Электронная информационно-образовательная среда ФГБОУ ВО «КЧГУ»

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) Университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории Университета, так и вне ее.

Функционирование ЭИОС обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование ЭИОС соответствует законодательству Российской Федерации.

Адрес официального сайта университета: http://kchgu.ru.

Адрес размещения ЭИОС ФГБОУ ВО «КЧГУ»: https://do.kchgu.ru.

Электронно-библиотечные системы (электронные библиотеки)

Учебный год	Наименование документа с указанием реквизитов	Срок действия документа
2024-2025 учебный год	Электронно-библиотечная система ООО «Знаниум». Договор № 238 от 23.04.2024г . Электронный адрес: https://znanium.com	от 23.04.2024г. до 11.05.2025г.
2024-2025 учебный год	Электронно-библиотечная система «Лань». Договор № 36 от 19.01.2024 г. Электронный адрес: https://e.lanbook.com	Бессрочный
2024-2025 учебный год	Электронно-библиотечная система КЧГУ. Положение об ЭБ утверждено Ученым советом от 30.09.2015г. Протокол № 1. Электронный адрес: http://lib.kchgu.ru	Бессрочный

2024-2025 учебный год	Национальная электронная библиотека (НЭБ). Договор №101/НЭБ/1391-п от 22. 02. 2023 г. Электронный адрес: http://rusneb.ru	Бессрочный
2024-2025 учебный год	Научная электронная библиотека «ELIBRARY.RU». Лицензионное соглашение №15646 от 21.10.2016 г. Электронный адрес: http://elibrary.ru	Бессрочный
2024-2025 учебный год	Электронный ресурс Polpred.comОбзор СМИ. Соглашение. Бесплатно. Электронный адрес: http://polpred.com	Бессрочный

9.2. Материально-техническое и учебно-методическое обеспечение дисциплины

Занятия проводятся в учебных аудиториях, предназначенных для проведения занятий лекционного и практического типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации в соответствии с расписанием занятий по образовательной программе. С описанием оснащенности аудиторий можно ознакомиться на сайте университета, в разделе материально-технического обеспечения и оснащенности образовательного процесса по адресу: https://kchgu.ru/sveden/objects/

9.3. 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), с 25.01.2023 г. по 03.03.2025 г.

9.4. Современные профессиональные базы данных и информационные справочные системы

1. Федеральный портал «Российское образование»- https://edu.ru/documents/
2. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) – http://school-collection.edu.ru/
3. Базы данных Scopus издательства Elsevirhttp://www.scopus.com/search/form.uri?display=basic.
4. Портал Федеральных государственных образовательных стандартов высшего образования - http://fgosvo.ru.
5. Федеральный центр информационно-образовательных ресурсов (ФЦИОР) –http://edu.ru.
6. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) – http://school-collection.edu.ru.
7. Информационная система «Единое окно доступа к образовательным ресурсам» (ИС «Единое окно») – http://window/edu.ru.

10. Особенности организации образовательного процесса для лиц с ограниченными возможностями здоровья

В ФГБОУ ВО «Карачаево-Черкесский государственный университет имени У.Д. Алиева» созданы условия для получения высшего образования по образовательным программам обучающихся с ограниченными возможностями здоровья (ОВЗ).

Специальные условия для получения образования по ОПВО обучающимися с ограниченными возможностями здоровья определены «Положением об обучении лиц с ОВЗ в КЧГУ», размещенным на сайте Университета по адресу: http://kchgu.ru.

11. Лист регистрации изменений

В рабочей программе внесены следующие изменения:

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