

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет компьютерных технологий и прикладной математики

УТВЕРЖДАЮ

Проректор по учебной работе,
качеству образования – первый
проректор

Хагуров Т.А.

подпись

«28» мая 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.33«Защита информации»

Направление подготовки 02.03.03 Математическое обеспечение и
администрирование информационных систем

Направленность (профиль) Технология программирования

Форма обучения очная

Квалификация бакалавр

Краснодар 2021

Рабочая программа дисциплины «Защита информации» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем.

Программу составил(и):

В.В. Подколзин, доцент, канд. физ.-мат. наук

И.О. Фамилия, должность, ученая степень, ученое звание



подпись

О.В. Гаркуша, доцент, канд. физ.-мат. наук, доцент

И.О. Фамилия, должность, ученая степень, ученое звание



подпись

Рабочая программа дисциплины «Защита информации» утверждена на заседании кафедры информационных технологий протокол №15 от «20» мая 2021 г.

Заведующий кафедрой (разработчика)

В. В. Подколзин



подпись

Рабочая программа обсуждена на заседании кафедры информационных технологий протокол №15 от «20» мая 2021 г.

Заведующий кафедрой (выпускающей)

В. В. Подколзин



подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол №1 от «21» мая 2021 г.

Председатель УМК факультета

А. В. Коваленко



подпись

Рецензенты:

Рубцов Сергей Евгеньевич, кандидат физико-математических наук, доцент кафедры математического моделирования ФГБГОУ «КубГУ»

Бегларян Маргарита Евгеньевна, кандидат физико-математических наук, доцент, заведующий кафедрой СГЕНД СКФ ФГБОУ ВО «Российский государственный университет правосудия»

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Курс посвящен изучению современных концепций информационной безопасности и их применения в обеспечении защиты информации и безопасного использования программных средств в вычислительных системах. Цель курса – научить студента методам информационной безопасности и их использованию в области защиты информации. Задачей курса является изложение теории информационной безопасности и практики применения алгоритмов криптозащиты.

Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению технологий, методов и средств производства и защиты программного обеспечения. Дать студентам математические основы защиты информации.

Отбор материала основывается на необходимости ознакомить студентов со следующей современной научной информацией:

- методы защиты информации;
- области применения защиты информации;
- о технологиях анализа шифров.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке бакалавра.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

Студент в рамках курса должен знать области применения задач информационной безопасности; методы защиты информации; области применения различных методов информационной безопасности; этапы, методы и инструментальные средства информационной безопасности; принципы построения и функционирования систем информационной безопасности; классификацию шифров; основы организации идентификации и цифровой подписи; принципы построения и применения паролей; уметь проводить анализ и определять оптимальный метод защиты информации; формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; формулировать и решать задачи организации процесса цифровой подписи; формулировать и решать задачи организации процесса идентификации; реализовать на языке программирования заданный метод защиты информации; решать задачи анализа шифра.

В качестве основной формы итогового контроля по рассматриваемой дисциплине предусмотрен зачет.

1.2 Задачи дисциплины

Основные задачи курса на основе системного подхода:

- иметь базовые знания по основам теории защиты информации;
- уметь на практике реализовывать различные методы надёжной и быстрой защиты информации;
- уметь при решении конкретной задачи профессионально грамотно сформулировать задачу передачи электронных данных;
- иметь базовые знания о методах передачи и защиты конфиденциальной информации;
- расширение практической базы для изучения других учебных дисциплин, таких, как "Технология разработки программного обеспечения", "Архитектура вычислительных и компьютерных систем" и др.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке бакалавра.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Защита информации» относится к «Обязательная часть» Блока 1 «Дисциплины (модули)» учебного плана.

Курс опирается на знания курсов «Математическая логика и дискретная математика», «Языки программирования и методы трансляции», «Основы сетевых технологий». Курс расширяет знания студентов в области создания программных систем, защиты данных и знаний.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

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

Знать ИУК-2.1 (С/16.6 Зн.1) Языки программирования и работы с базами данных, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.2 (С/16.6 Зн.3) Инструменты и методы верификации структуры программного кода, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.16 (А/01.5 Зн.1) Цели и задачи проводимых исследований и разработок в рамках поставленной цели, методы выбора оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.18 (А/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Уметь ИУК-2.19 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.20 (А/01.5 У.1) Применять нормативную документацию в соответствующей области знаний, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.21 (А/01.5 У.3) Применять методы анализа научно-технической информации, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Владеть ИУК-2.27 (А/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта, в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ОПК-2 Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества

программных продуктов и программных комплексов в различных областях человеческой деятельности

- Знать**
- ИОПК-2.1 (D/03.6 Зн.3) Методы и средства проектирования программного обеспечения, оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры и оценки качества программного кода
 - ИОПК-2.3 (C/16.6 Зн.4) Возможности ИС в различных областях человеческой деятельности
 - ИОПК-2.4 (C/16.6 Зн.8) Основы программирования, проектирования, разработки, реализации и оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.5 (C/16.6 Зн.14) Современный отечественный и зарубежный опыт, современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.6 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.7 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.8 (A/01.5 Зн.4) Методы проведения экспериментов и наблюдений, обобщения и обработки информации, связанной с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.9 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач на основе современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
- Уметь**
- ИОПК-2.10 (C/16.6 У.2) Верифицировать структуру программного кода, применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.11 (A/27.6 У.1) Анализировать входные данные, применять современный математический аппарат, связанный с проектированием, разработкой и реализацией программных продуктов и программных комплексов в различных областях человеческой деятельности
- Владеть**
- ИОПК-2.13 (C/16.6 Тд.2) Верификация структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС, оценка качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.15 (A/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта при разработке программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.16 (А/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в соответствующей области знаний, использование современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

- ПК-1** **Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий**
- Знать**
- ИПК-1.1 (D/03.6 Зн.2) Типовые решения, математические модели, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения
 - ИПК-1.3 (С/16.6 Зн.2) Инструменты и методы проектирования и дизайна ИС
 - ИПК-1.4 (С/16.6 Зн.5) Предметная область автоматизации
 - ИПК-1.5 (С/16.6 Зн.8) Основы программирования и информационных технологий
 - ИПК-1.8 (А/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта в области знания математических и естественных наук, программирования и информационных технологий
 - ИПК-1.9 (А/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок в области знания математических и естественных наук, программирования и информационных технологий
 - ИПК-1.10 (А/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач в области знания математических и естественных наук, программирования и информационных технологий
- Уметь**
- ИПК-1.11 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения на основе знаний и моделей математических и естественных наук
 - ИПК-1.13 (А/27.6 У.1) Анализировать входные данные
 - ИПК-1.14 (А/01.5 У.3) Применять методы анализа научно-технической информации с использованием базовых знаний математических и естественных наук, программирования и информационных технологий
- Владеть**
- ИПК-1.15 (D/03.6 Тд.2) Проектирование структур данных, построение математических моделей
 - ИПК-1.16 (А/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в области знаний математических и естественных наук, программирования и информационных технологий

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72 часов), их распределение по видам работ представлено в таблице

Вид учебной работы	Всего часов	Семестры (часы)					
		8					
Контактная работа, в том числе:	30,2	30,2					
Аудиторные занятия (всего):	28	28					
Занятия лекционного типа							
Лабораторные занятия	28	28					
Занятия семинарского типа (семинары, практические занятия)							
Иная контактная работа:	2,2	2,2					
Контроль самостоятельной работы (КСР)	2	2					
Промежуточная аттестация (ИКР)	0,2	0,2					
Самостоятельная работа, в том числе:	41,8	41,8					
<i>Курсовая работа</i>							
<i>Проработка учебного (теоретического) материала</i>							
<i>Выполнение индивидуальных заданий (подготовка сообщений, презентаций)</i>							
<i>Реферат</i>							
Подготовка к текущему контролю							
Контроль:							
Подготовка к экзамену							
Общая трудоемкость	час.	72	72				
	в том числе контактная работа	30,2	30,2				
	зач. ед	2	2				

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 8 семестре

№	Наименование разделов (тем)	Всего	Количество часов			Внеаудиторная работа СРС
			Аудиторная работа			
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1.	Основы теории защиты информации					
2.	Линейное и нелинейное кодирование. Корректирующие свойства кодов					
3.	Конечные поля					
4.	Обнаружение и исправление ошибок					
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
14.						
ИТОГО по разделам дисциплины					28	
Контроль самостоятельной работы (КСР)		2				
Промежуточная аттестация (ИКР)		0,2				
Подготовка к текущему контролю						
Общая трудоемкость по дисциплине		72				

Примечание: Л – лекции, ПЗ – практические занятия/семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

Не предусмотрены

Примечание: ЛР – отчет/защита лабораторной работы, КП – выполнение курсового проекта, КР – курсовой работы, РГЗ – расчетно-графического задания, Р – написание реферата, Э – эссе, К – коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.2 Занятия семинарского типа

Не предусмотрены

Примечание: ЛР – отчет/защита лабораторной работы, КП – выполнение курсового проекта, КР – курсовой работы, РГЗ – расчетно-графического задания, Р – написание реферата, Э – эссе, К – коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.3 Лабораторные занятия

№	Наименование раздела (темы)	Наименование лабораторных работ	Форма текущего контроля
1	2	3	4
1.	Теория информации и её энтропия	Различные подходы. Сравнение неопределённостей. Примеры	
2.	Количественная мера по Хартли, по Шеннону и А.Н. Колмогорову	Мера неопределённости информации. Количество информации и его свойства	
3.	Алфавит дискретных логических устройств	Простые конечные поля и их свойства. Конечное поле GF(q) и его свойства	
4.	Теория кодирования	Примеры кодов. Коды Хэмминга. Совершенство кодов Хэмминга	
5.	Циклические коды	Описание циклических кодов. AN-циклические коды и их свойства	

№	Наименование раздела (темы)	Наименование лабораторных работ	Форма текущего контроля
1	2	3	4
6.	Коды БЧХ, исправляющие две ошибки	Обобщение линейных кодов. Обнаружение и исправление двух симметричных ошибок	
7.	Матрицы Адамара. Нелинейные коды.	Существование матриц Адамара. Коды Адамара	
8.	Границы мощности кодов	Граница сферической упаковки. Граница Р.Р. Варшамова и др.	
9.			
10.			
11.			
12.			
13.			
14.			

Примечание: ЛР – отчет/защита лабораторной работы, КП - выполнение курсового проекта, КР - курсовой работы, РГЗ - расчетно-графического задания, Р - написание реферата, Э - эссе, К - коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы - не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Изучение теоретического материала	Методические указания по организации самостоятельной работы студентов, утвержденные кафедрой информационных технологий, протокол №1 от 30.08.2019
2	Решение задач	Методические указания по организации самостоятельной работы студентов, утвержденные кафедрой информационных технологий, протокол №1 от 30.08.2019

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,

- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В соответствии с требованиями ФГОС в программа дисциплины предусматривает использование в учебном процессе следующих образовательные технологии: чтение лекций с использованием мультимедийных технологий; метод малых групп, разбор практических задач и кейсов.

При обучении используются следующие образовательные технологии:

- Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.

- Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал. Создание и использование диагностических тестов является неотъемлемой частью данной технологии.

- Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.

- Информационно-коммуникационные технологии (ИКТ) - расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют интенсификации самостоятельной работы учащихся и повышению познавательной активности. В рамках ИКТ выделяются 2 вида технологий:

- Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения языку на всех уровнях.

- Интернет-технологии – предоставляют широкие возможности для поиска информации, разработки научных проектов, ведения научных исследований.

- Технология индивидуализации обучения – помогает реализовывать личностно-ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.

- Проектная технология – ориентирована на моделирование социального взаимодействия учащихся с целью решения задачи, которая определяется в рамках профессиональной подготовки, выделяя ту или иную предметную область.

- Технология обучения в сотрудничестве – реализует идею взаимного обучения, осуществляя как индивидуальную, так и коллективную ответственность за решение учебных задач.

- Игровая технология – позволяет развивать навыки рассмотрения ряда возможных способов решения проблем, активизируя мышление студентов и раскрывая личностный потенциал каждого учащегося.

- Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Комплексное использование в учебном процессе всех вышеназванных технологий стимулируют личностную, интеллектуальную активность, развивают познавательные процессы, способствуют формированию компетенций, которыми должен обладать будущий специалист.

Основные виды интерактивных образовательных технологий включают в себя:

- работа в малых группах (команде) - совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путём творческого сложения

результатов индивидуальной работы членов команды с делением полномочий и ответственности;

– проектная технология - индивидуальная или коллективная деятельность по отбору, распределению и систематизации материала по определенной теме, в результате которой составляется проект;

– анализ конкретных ситуаций - анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений;

– развитие критического мышления – образовательная деятельность, направленная на развитие у студентов разумного, рефлексивного мышления, способного выдвинуть новые идеи и увидеть новые возможности.

Подход разбора конкретных задач и ситуаций широко используется как преподавателем, так и студентами во время лекций, лабораторных занятий и анализа результатов самостоятельной работы. Это обусловлено тем, что при исследовании и решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	количество интерактивных часов
	Л, ЛР, ПЗ	Практические занятия в режимах взаимодействия «преподаватель – студент» и «студент – студент»	8
Итого			8

Примечание: Л – лекции, ПЗ – практические занятия/семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Темы, задания и вопросы для самостоятельной работы призваны сформировать навыки поиска информации, умения самостоятельно расширять и углублять знания, полученные в ходе лекционных и практических занятий.

Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. Оценочные и методические материалы

4.1 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «название дисциплины».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме **тестовых заданий, доклада-презентации по проблемным вопросам, разноуровневых заданий, ролевой игры, ситуационных задач (указать иное) и промежуточной аттестации** в форме **вопросов и заданий (указать иное) к экзамену (дифференцированному зачету, зачету).**

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Структура оценочных средств для текущей и промежуточной аттестации

Перечень заданий текущего контроля по темам:

1. Коды Варшамова. Обнаружение и исправление несимметричных одиночных ошибок.
Примеры
2. Квадратично-вычетные коды. Граница квадратичного корня
3. Корректирующие возможности арифметических AN-кодов
4. Методы комбинирования кодов.
5. Доказать, что каждый ненулевой элемент поля $GF(P)$ имеет обратный элемент
6. Определить число примитивных элементов поля $GF(P)$
7. Доказать, что для произвольных двух элементов $a, b \in GF(P)$ имеет место равенство $(a + b)^P = a^P + b^P$
8. Доказать, что $(P - 1)! = -1$
9. Доказать, что если $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n, a_n \in GF(P)$, то $f(x^P) = (f(x))^P$
10. Доказать, что корнями уравнения $x^P - x = 0$ являются все элементы поля $GF(P)$
11. Найти число $N_P(a x + b)$ всех линейных функций $y = a x + b$ в $GF(P)$

12. Найти число $N_P((ax + b)/(cx + d))$ всех дробно - линейных функций $y = (ax + b)/(cx + d)$ в $GF(P)$
13. Определить число $N_P(ad - bc = k)$ в $GF(P)$, где $k \in GF(P)$
14. Найти число решений $N_P(x_1 + x_2 + \dots + x_n = k)$ уравнения $x_1 + x_2 + \dots + x_n = k$ в $GF(P)$, где $k \in GF(P)$
15. Доказать, что $x^P - x = F_1(x) F_P(x)$, где $F_1(x)$ и $F_P(x)$ произведения всех простых над $GF(P)$ полиномов степеней 1 и P соответственно
16. Определить число $I_P(n)$ простых над $GF(P)$ полиномов степени n . Доказать, что $I_P(n) \geq 1$
17. Разработать алгоритм построения простого над $GF(P)$ полиномов заданной степени в явном виде

Показатели, критерии и шкала оценки сформированных компетенций

Соответствие **пороговому уровню** освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **удовлетворительно /зачтено**):

- | | |
|----------------|---|
| 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 |
| Знать | <p>ИУК-2.1 (С/16.6 Зн.1) Языки программирования и работы с базами данных, исходя из действующих правовых норм, имеющихся ресурсов и ограничений</p> <p>ИУК-2.2 (С/16.6 Зн.3) Инструменты и методы верификации структуры программного кода, исходя из действующих правовых норм, имеющихся ресурсов и ограничений</p> <p>ИУК-2.16 (А/01.5 Зн.1) Цели и задачи проводимых исследований и разработок в рамках поставленной цели, методы выбора оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений</p> <p>ИУК-2.18 (А/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений</p> |
| Уметь | <p>ИУК-2.19 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений</p> <p>ИУК-2.20 (А/01.5 У.1) Применять нормативную документацию в соответствующей области знаний, исходя из действующих правовых норм, имеющихся ресурсов и ограничений</p> <p>ИУК-2.21 (А/01.5 У.3) Применять методы анализа научно-технической информации, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений</p> |
| Владеть | ИУК-2.27 (А/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта, в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений |
| ОПК-2 | Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности |

- Знать**
- ИОПК-2.1 (D/03.6 Зн.3) Методы и средства проектирования программного обеспечения, оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры и оценки качества программного кода
 - ИОПК-2.3 (C/16.6 Зн.4) Возможности ИС в различных областях человеческой деятельности
 - ИОПК-2.4 (C/16.6 Зн.8) Основы программирования, проектирования, разработки, реализации и оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.5 (C/16.6 Зн.14) Современный отечественный и зарубежный опыт, современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.6 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.7 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.8 (A/01.5 Зн.4) Методы проведения экспериментов и наблюдений, обобщения и обработки информации, связанной с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.9 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач на основе современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
- Уметь**
- ИОПК-2.10 (C/16.6 У.2) Верифицировать структуру программного кода, применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.11 (A/27.6 У.1) Анализировать входные данные, применять современный математический аппарат, связанный с проектированием, разработкой и реализацией программных продуктов и программных комплексов в различных областях человеческой деятельности
- Владеть**
- ИОПК-2.13 (C/16.6 Тд.2) Верификация структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС, оценка качества программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.15 (A/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта при разработке программных продуктов и программных комплексов в различных областях человеческой деятельности
 - ИОПК-2.16 (A/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в соответствующей области знаний,

использование современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ПК-1 Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий

Знать ИПК-1.1 (D/03.6 Зн.2) Типовые решения, математические модели, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения

ИПК-1.3 (C/16.6 Зн.2) Инструменты и методы проектирования и дизайна ИС

ИПК-1.4 (C/16.6 Зн.5) Предметная область автоматизации

ИПК-1.5 (C/16.6 Зн.8) Основы программирования и информационных технологий

ИПК-1.8 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.9 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.10 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач в области знания математических и естественных наук, программирования и информационных технологий

Уметь ИПК-1.11 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения на основе знаний и моделей математических и естественных наук

ИПК-1.13 (A/27.6 У.1) Анализировать входные данные

ИПК-1.14 (A/01.5 У.3) Применять методы анализа научно-технической информации с использованием базовых знаний математических и естественных наук, программирования и информационных технологий

Владеть ИПК-1.15 (D/03.6 Тд.2) Проектирование структур данных, построение математических моделей

ИПК-1.16 (A/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в области знаний математических и естественных наук, программирования и информационных технологий

Соответствие **базовому уровню** освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **хорошо /зачтено**):

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

Знать ИУК-2.1 (C/16.6 Зн.1) Языки программирования и работы с базами данных, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры программного кода, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.16 (A/01.5 Зн.1) Цели и задачи проводимых исследований и разработок в рамках поставленной цели, методы выбора оптимальных способов их

решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.18 (А/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

- Уметь** ИУК-2.19 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- ИУК-2.20 (А/01.5 У.1) Применять нормативную документацию в соответствующей области знаний, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- ИУК-2.21 (А/01.5 У.3) Применять методы анализа научно-технической информации, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

- Владеть** ИУК-2.27 (А/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта, в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ОПК-2 **Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности**

- Знать** ИОПК-2.1 (D/03.6 Зн.3) Методы и средства проектирования программного обеспечения, оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности
- ИОПК-2.2 (С/16.6 Зн.3) Инструменты и методы верификации структуры и оценки качества программного кода
- ИОПК-2.3 (С/16.6 Зн.4) Возможности ИС в различных областях человеческой деятельности
- ИОПК-2.4 (С/16.6 Зн.8) Основы программирования, проектирования, разработки, реализации и оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности
- ИОПК-2.5 (С/16.6 Зн.14) Современный отечественный и зарубежный опыт, современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
- ИОПК-2.6 (А/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
- ИОПК-2.7 (А/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок программных продуктов и программных комплексов в различных областях человеческой деятельности
- ИОПК-2.8 (А/01.5 Зн.4) Методы проведения экспериментов и наблюдений, обобщения и обработки информации, связанной с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.9 (А/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач на основе современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

Уметь ИОПК-2.10 (С/16.6 У.2) Верифицировать структуру программного кода, применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.11 (А/27.6 У.1) Анализировать входные данные, применять современный математический аппарат, связанный с проектированием, разработкой и реализацией программных продуктов и программных комплексов в различных областях человеческой деятельности

Владеть ИОПК-2.13 (С/16.6 Тд.2) Верификация структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС, оценка качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.15 (А/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта при разработке программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.16 (А/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в соответствующей области знаний, использование современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ПК-1 **Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий**

Знать ИПК-1.1 (D/03.6 Зн.2) Типовые решения, математические модели, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения

ИПК-1.3 (С/16.6 Зн.2) Инструменты и методы проектирования и дизайна ИС

ИПК-1.4 (С/16.6 Зн.5) Предметная область автоматизации

ИПК-1.5 (С/16.6 Зн.8) Основы программирования и информационных технологий

ИПК-1.8 (А/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.9 (А/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.10 (А/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач в области знания математических и естественных наук, программирования и информационных технологий

- Уметь** ИПК-1.11 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения на основе знаний и моделей математических и естественных наук
ИПК-1.13 (A/27.6 У.1) Анализировать входные данные
ИПК-1.14 (A/01.5 У.3) Применять методы анализа научно-технической информации с использованием базовых знаний математических и естественных наук, программирования и информационных технологий
- Владеть** ИПК-1.15 (D/03.6 Тд.2) Проектирование структур данных, построение математических моделей
ИПК-1.16 (A/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в области знаний математических и естественных наук, программирования и информационных технологий

Соответствие **продвинутому уровню** освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **отлично /зачтено**):

- 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**
- Знать** ИУК-2.1 (C/16.6 Зн.1) Языки программирования и работы с базами данных, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры программного кода, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.16 (A/01.5 Зн.1) Цели и задачи проводимых исследований и разработок в рамках поставленной цели, методы выбора оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.18 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- Уметь** ИУК-2.19 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.20 (A/01.5 У.1) Применять нормативную документацию в соответствующей области знаний, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.21 (A/01.5 У.3) Применять методы анализа научно-технической информации, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- Владеть** ИУК-2.27 (A/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта, в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- ОПК-2** **Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества**

программных продуктов и программных комплексов в различных областях человеческой деятельности

Знать

ИОПК-2.1 (D/03.6 Зн.3) Методы и средства проектирования программного обеспечения, оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры и оценки качества программного кода

ИОПК-2.3 (C/16.6 Зн.4) Возможности ИС в различных областях человеческой деятельности

ИОПК-2.4 (C/16.6 Зн.8) Основы программирования, проектирования, разработки, реализации и оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.5 (C/16.6 Зн.14) Современный отечественный и зарубежный опыт, современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.6 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.7 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.8 (A/01.5 Зн.4) Методы проведения экспериментов и наблюдений, обобщения и обработки информации, связанной с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.9 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач на основе современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

Уметь

ИОПК-2.10 (C/16.6 У.2) Верифицировать структуру программного кода, применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.11 (A/27.6 У.1) Анализировать входные данные, применять современный математический аппарат, связанный с проектированием, разработкой и реализацией программных продуктов и программных комплексов в различных областях человеческой деятельности

Владеть

ИОПК-2.13 (C/16.6 Тд.2) Верификация структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС, оценка качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.15 (A/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта при разработке программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.16 (А/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в соответствующей области знаний, использование современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

- ПК-1** **Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий**
- Знать**
- ИПК-1.1 (D/03.6 Зн.2) Типовые решения, математические модели, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения
 - ИПК-1.3 (С/16.6 Зн.2) Инструменты и методы проектирования и дизайна ИС
 - ИПК-1.4 (С/16.6 Зн.5) Предметная область автоматизации
 - ИПК-1.5 (С/16.6 Зн.8) Основы программирования и информационных технологий
 - ИПК-1.8 (А/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта в области знания математических и естественных наук, программирования и информационных технологий
 - ИПК-1.9 (А/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок в области знания математических и естественных наук, программирования и информационных технологий
 - ИПК-1.10 (А/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач в области знания математических и естественных наук, программирования и информационных технологий
- Уметь**
- ИПК-1.11 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения на основе знаний и моделей математических и естественных наук
 - ИПК-1.13 (А/27.6 У.1) Анализировать входные данные
 - ИПК-1.14 (А/01.5 У.3) Применять методы анализа научно-технической информации с использованием базовых знаний математических и естественных наук, программирования и информационных технологий
- Владеть**
- ИПК-1.15 (D/03.6 Тд.2) Проектирование структур данных, построение математических моделей
 - ИПК-1.16 (А/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в области знаний математических и естественных наук, программирования и информационных технологий

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

(Указать перечень заданий, круглый столов, кейсов при текущей аттестации, с указанием кодов оцениваемых компетенций)

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

Список задач и вопросов для подготовки к промежуточной аттестации

Список вопросов для подготовки к зачету

1. Информация и неопределённость. Количественная мера неопределённости. Подходы Р. Хартли, К. Шеннона и А.Н. Колмогорова
2. Алфавит дискретных устройств. Конечные поля
3. Простое поле Галуа $GF(P)$. Составное поле Галуа $GF(P^n)$
4. Математические методы защиты информации от помех в каналах связи
5. Кодирование информации. Основные понятия. Примеры
6. Линейные коды. Способы их задания
7. Свойства линейного кода. Коды Хэмминга
8. Граница Хэмминга. Граница Варшавова-Гильберта
9. Коды Варшавова. Обнаружение и исправление несимметричных одиночных ошибок
10. Циклические коды и их описание
11. Коды БЧХ, исправляющие две ошибки
12. Нелинейные коды. Коды Адамара
13. Совершенные коды. Двоичный код Голея
14. Квадратично-вычетные коды. Граница квадратичного корня
15. Арифметические АН-коды и их свойства
16. Корректирующие возможности арифметических АН-кодов
17. Коды Рида-Соломона и их корректирующие возможности
18. Коды Рида-Маллера и их корректирующие возможности
19. Методы комбинирования кодов
20. Повышение надёжности цифровых устройств с помощью корректирующих кодов
21. Границы мощности кодов
22. Информация и неопределённость
23. Количественная мера неопределённости
24. Условная неопределённость. Количество информации
25. Передача информации
26. Пропускная способность канала связи. Теоремы Шеннона
27. Сжатие информации. Метод Шеннона-Фано

Примерные задачи для подготовки к зачету

1. Доказать, что два поля Галуа с одним и тем же числом элементов изоморфны
2. Доказать, что над каждым полем $GF(q)$ существует примитивный полином любой положительной степени.
3. Пусть $x = x_1 x_2 \dots x_n$, $y = y_1 y_2 \dots y_n \in GF(2^n)$. Установить связь между расстояниями Хэмминга $d_X(x, y)$ и Евклида $d_E(x, y)$
4. Доказать, что для расстояния Хэмминга выполняется неравенство треугольника $d(x, y) \leq d(x, z) + d(z, y)$
5. Доказать, что $Hx^t = 0$ тогда и только тогда, когда шумовое слово равно нулю
6. Для фиксированной длины n определить наименьшее число избыточных символов
7. Доказать, что если $H = (A | Er)$, то $G = (Ek | -A^t k)$
8. Доказать, что $d(x, y) = d(x + z, y + z) = W(x + y)$
9. Разработать алгоритм декодирования линейных блочных кодов
10. Доказать, что код с кодовым расстоянием d может исправлять $\lfloor (d-1)/2 \rfloor$ ошибок, причём если d чётное, то он может одновременно исправлять $(d-1)/2$ ошибок и обнаруживать $d/2$ ошибок
11. Доказать, что если H - проверочная матрица линейного кода длины n , то код имеет минимальное расстояние d тогда и только тогда, когда любые $d-1$ столбцов матрицы H линейно независимы, но найдутся d линейно зависимых столбцов

12. Доказать, что если i, j, \dots, k - номера ошибочных позиций принятого слова x' некоторого линейного кода с проверочной матрицей H , то $S = Hx' = H_i + H_j + \dots + H_k$, где H_i - i -й столбец матрицы H
13. Доказать, что кодовое расстояние кодов Хэмминга равно 3
14. Доказать, что кодовое расстояние расширенных кодов Хэмминга равно 4
15. Построить проверочную матрицу $[13, 10, 3]$ - кода Хэмминга над полем $GF(3)$
16. Доказать, что если C - двоичный линейный код и слово $a \notin C$, то $CU(a+C)$ также является двоичным линейным кодом
17. 1
18. Доказать, что если C является $[n, k, d]$ - кодом над полем $GF(P)$, то множество всех слов $GF_n(P)$ можно разбить на непересекающиеся смежные классы: $GF_n(P) = C \cup (a_1 + C) \cup (a_2 + C) \cup \dots \cup (a_t + C)$, где $t = P^{n-k-1}$
19. Доказать, что если $C = [n, k, d]$ - код, то $d \leq n - k + 1$ (Граница Синглтона)
20. Определить веса всех кодовых слов (спектр весов) кода H_7 .

4.2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Компонентом промежуточного контроля по дисциплине являются решение задачи из списка задач к промежуточной аттестации и ответа на два теоретических вопроса. Максимальное количество баллов, которые студент может получить за ответ вопрос, составляет 6 баллов. Максимальное количество баллов, которые студент может получить за правильное решение задачи составляет 3 балла.

Количество баллов, которое студенты могут получить за выполнение заданий определяется согласно таблицы:

Описание	Баллы
<i>Вопрос</i>	
Студент владеет теоретическими знаниями по данному вопросу, что подтверждается его ответами на дополнительные вопросы; студент умеет правильно объяснять теоретический материал, иллюстрируя его примерами;	5-6
Студент владеет теоретическими знаниями по данному вопросу, при ответе студент допускает незначительные ошибки; студент умеет правильно объяснять теоретический материал;	3-4
Теоретический материал не усвоен или усвоен частично, студент не может предоставить четкий ответ на поставленный вопрос; студент затрудняется привести примеры, поясняющие ответы на вопросы;	0-2
<i>Задача</i>	
Задача решена правильно, студент может пояснить ход решения	2
Задача решена неправильно, однако решение задачи показывает, что студент понимает материал, студент может пояснить ход решения,	1
Задача решена неправильно, решение задачи показывает, что студент не понимает материал	0

Критерии оценки:

Оценка	
Незачет	Зачтено
<ul style="list-style-type: none"> • студент получил 0 баллов за задачу и менее 5 баллов по каждому из двух вопросов 	<ul style="list-style-type: none"> • студент получил не менее 1 балла за задачу и не менее 3 баллов за один из двух вопросов;

Оценка	
Незачет	Зачтено
	<ul style="list-style-type: none"> • студент получил не менее 4 балла за задачу; • студент получил не менее 1 балла за задачу и не менее 5 баллов за один из двух вопросов • студент получил не менее 2 баллов за задачу и не менее 5 баллов за один из двух вопросов; студент получил не менее 10 баллов за два вопроса студент получил 3 балла за задачу и не менее 11 баллов за два вопроса, ответил на дополнительные вопросы

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1 Основная литература:

1. Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Е. К. Баранова, А. В. Бабаш . - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017. - 322 с. - <http://znanium.com/catalog.php?bookinfo=763644>
2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - <http://biblioclub.ru/index.php?page=book&id=438331>.
3. Лапониная, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия [Текст] : учебное пособие для студентов вузов / О. Р. Лапониная ; [под ред. В. А. Сухомлина]. - 2-е изд., испр. - М. : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний , 2007.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература:

1. Бабаш, А. В. Криптографические методы защиты информации [Текст] : учебник для студенто вузов, обучающихся по направлению "Прикладная информатика" / А. В. Бабаш, Е. К. Баранова. - Москва : КНОРУС, 2016. - 189 с
2. Корт, С. С. Теоретические основы защиты информации [Текст] : учебное пособие для студентов вузов / С. С. Корт. - М. : Гелиос АРВ , 2004. - 233 с
3. Бабенко, Л.К. Параллельные алгоритмы для решения задач защиты информации [Электронный ресурс] : учебное пособие / Л.К. Бабенко, Е.А. Ищукова, И.Д. Сидоров. — Электрон. дан. — Москва : Горячая линия-Телеком, 2014. — 304 с. — Режим доступа: <https://e.lanbook.com/book/63228>
4. В.О. Осипян, К.В. Осипян Математические основы теории и практики защиты информации [Текст] : учебное пособие / В. О. Осипян, К. В. Осипян ; М-во образования Рос. Федерации, Кубанский гос. ун-т. - Краснодар : [КубГУ], 2003.
5. Осипян В.О. Разработка методов построения систем передачи и защиты информации [Текст] / В. О. Осипян ; М-во образования и науки Рос. Федерации, Кубанский гос. ун-т. - Краснодар : [КубГУ], 2004. - 179 с.

5.3. Периодические издания:

1. Базы данных компании «Ист Вью» <http://dlib.eastview.com>
2. Электронная библиотека GREBENNIKON.RU <https://grebennikon.ru/>
- 3.

5.4. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы
Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» <https://urait.ru/>
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» <https://www.book.ru>
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» <https://e.lanbook.com>

5.5.Профессиональные базы данных:

1. Web of Science (WoS) <http://webofscience.com/>
2. Scopus <http://www.scopus.com/>
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley <https://onlinelibrary.wiley.com/>
5. Научная электронная библиотека (НЭБ) <http://www.elibrary.ru/>
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН <http://archive.neicon.ru>
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) <https://rusneb.ru/>
8. Президентская библиотека им. Б.Н. Ельцина <https://www.prilib.ru/>
9. Электронная коллекция Оксфордского Российского Фонда <https://ebookcentral.proquest.com/lib/kubanstate/home.action>
10. Springer Journals <https://link.springer.com/>
11. Nature Journals <https://www.nature.com/siteindex/index.html>

12. Springer Nature Protocols and Methods
<https://experiments.springernature.com/sources/springer-protocols>
13. Springer Materials <http://materials.springer.com/>
14. zbMath <https://zbmath.org/>
15. Nano Database <https://nano.nature.com/>
16. Springer eBooks: <https://link.springer.com/>
17. "Лекториум ТВ" <http://www.lektorium.tv/>
18. Университетская информационная система РОССИЯ <http://uisrussia.msu.ru>

5.6. Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

5.7. ресурсы свободного доступа:

1. Американская патентная база данных <http://www.uspto.gov/patft/>
2. Полные тексты канадских диссертаций <http://www.nlc-bnc.ca/thesescanada/>
3. КиберЛенинка (<http://cyberleninka.ru/>);
4. Министерство науки и высшего образования Российской Федерации
<https://www.minobrnauki.gov.ru/>;
5. Федеральный портал "Российское образование" <http://www.edu.ru/>;
6. Информационная система "Единое окно доступа к образовательным ресурсам"
<http://window.edu.ru/>;
7. Единая коллекция цифровых образовательных ресурсов <http://school-collection.edu.ru/> .
8. Федеральный центр информационно-образовательных ресурсов (<http://fcior.edu.ru/>);
9. Проект Государственного института русского языка имени А.С. Пушкина
"Образование на русском" <https://pushkininstitute.ru/>;
10. Справочно-информационный портал "Русский язык" <http://gramota.ru/>;
11. Служба тематических толковых словарей <http://www.glossary.ru/>;
12. Словари и энциклопедии <http://dic.academic.ru/>;
13. Образовательный портал "Учеба" <http://www.ucheba.com/>;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--plai/voprosy_i_otvety

5.8. Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения <http://moodle.kubsu.ru>
2. База учебных планов, учебно-методических комплексов, публикаций и конференций
<http://mschool.kubsu.ru/>
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий <http://mschool.kubsu.ru;>
4. Электронный архив документов КубГУ <http://docspace.kubsu.ru/>
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ"
<http://icdau.kubsu.ru/>

6. Методические указания для обучающихся по освоению дисциплины (модуля)

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

№	Вид работ	Наименование учебной аудитории, ее оснащенность оборудованием и техническими средствами обучения
1.	Лекционные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения
2.	Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, проектором, программным обеспечением
3.	Практические занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения
4.	Групповые (индивидуальные) консультации	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
5.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
6.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

Примечание: Конкретизация аудиторий и их оснащение определяется ОПОП.