МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО Руководитель ОПОП	УТВЕРЖДАЮ Зав. кафедрой ПМИ
_____М.В. Коломина	_____М.В. Коломина
«8» сентября 2022 г.	«8» сентября 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Теория кодирования»

Составители	**Корнеев Г.А., к.т.н., доцент ФИТиП, ИТМО** **Кудряшов Б.Д., д.т.н., профессор, ИТМО**
Направление подготовки / специальность	**01.03.02 Прикладная математика и информатика**
Направленность (профиль) ОПОП	**Программирование и искусственный интеллект**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приёма	**2023**
Курс	**4**
Семестр(ы)	**7**

Астрахань – 2022

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины «Теория кодирования» являются

- формирование систематических знаний в области методов повышения надежности хранения и передачи данных;
- ознакомление с перспективными направлениями в области проектирования высоконадежных вычислительных систем;
- обучение вопросам построения эффективных кодов, используемых для обнаружения и исправления ошибок в кодовых комбинациях;
- выработка умения пользоваться разного рода справочными материалами и пособиями, самостоятельно расширяя математические знания, необходимые для решения практических задач.

1.2. Задачи освоения дисциплины:

- изучение методов сжатия цифровых данных, шаблонов проектирования ПО, используемых в промышленной разработке ПО, инструментов для профилирования разработанного кода под существующей нагрузкой сервиса;

- развитие практических навыков написания кода в рамках заданного в проекте стиля написания кода, осуществления перебора кодовой информации для декодирования данных в отсутствии кодовых значений.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина «Теория кодирования» относится к части, формируемой участниками образовательных отношений и осваивается в 7 семестре.

2.2. Для изучения данной учебной дисциплины необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами:

Математическая логика,

Дискретная математика

Криптография

Знания: основ математической логики, комбинаторики, теории графов, основных основные понятия дискретной математики, принципы передачи и хранения информации, а также о мерах информации, основных угроз безопасности информации и методов защиты данных

Умения: определять угрозы информационной безопасности, применять математические методы для решения типовых задач, составлять алгоритмы, с использованием основных алгоритмических структур.

Навыки: критического мышления, анализировать сложные проблемы, связанные с безопасностью данных, и находить оптимальные решения

2.3. Последующие учебные дисциплины и практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной.

Проектирование программного обеспечения

Преддипломная практика, ВКР.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки / специальности:

а) профессиональных (ПК).

- ПК-3. Способен обеспечивать заданный уровень производительности, надежности и безопасности при создании вариантов архитектуры программного средства.
- ПК-8. Способность понимать, совершенствовать и применять современный математический аппарат.

Таблица 1 – Декомпозиция результатов обучения

Код компетенции	Планируемые результаты освоения дисциплины (модуля)		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-3	ИПК-3.1.1. Методы сжатия цифровых данных, шаблоны проектирования ПО, используемые в промышленной разработке ПО, инструменты для профилирования разработанного кода под существующей нагрузкой сервиса	ИПК-3.2.1. Читать код, соответствующий стилю кода в проекте	ИПК-3.3.1 Навыком написания кода в рамках заданного в проекте стиля написания кода, осуществлять перебор кодовой информации для декодирования данных в отсутствии кодовых значений
ПК-8	ИПК-8.1.1. Современный математический аппарат	ИПК-8.2.1. Навыками применения современного математического аппарата	ИПК-8.3.1. Методами функционального анализа для решения сложных задач информатики

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Объем дисциплины составляет 5 зачетных единиц, в том числе 60 часов, выделенных на контактную работу обучающихся с преподавателем (из них 30 часов – лекции, 30 часов – лабораторные работы) и 120 часов – на самостоятельную работу обучающихся.

Таблица 2 – Структура и содержание дисциплины

№ п/п	Наименование раздела, темы	Семестр	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости Форма промежуточной аттестации
			Л	ПЗ	ЛР	КР	СР	
1	Линейные коды	7	7		8		30	Лабораторная работа №1
2	БЧХ/РС коды	7	8		7		30	Лабораторная работа №2
3	Сверточные коды	7	8		7		30	Лабораторная работа №3
4	Коды с малой плотностью проверок на четность	7	7		8		30	Лабораторная работа №4
ИТОГО			**30**		**30**		**120**	**Экзамен**

Таблица 3 – Матрица соотнесения разделов, тем учебной дисциплины и формируемых в них компетенций

Разделы, темы дисциплины (модуля)	Кол-во часов	Компетенции		
		ПК-3	ПК-8	Общее количество компетенций
Раздел 1. Линейные коды	45	+	+	2
Раздел 2. БЧХ/РС коды	45	+	+	2
Раздел 3. Сверточные коды	45	+	+	2
Раздел 4. Коды с малой плотностью проверок на четность	45	+	+	2

Краткое содержание каждой темы дисциплины (модуля)

№ раздела	Наименование раздела дисциплины	Содержание
1	Линейные коды	Линейные коды
2	БЧХ/РС коды	БЧХ/РС коды
3	Сверточные коды	Сверточные коды
4	Коды с малой плотностью проверок на четность	Коды с малой плотностью проверок на четность

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

Лекционные занятия

Основной формой реализации теоретического обучения является лекция, которая представляет собой систематическое, последовательное изложение преподавателем-лектором учебного материала теоретического характера. Цель лекции – организация целенаправленной познавательной деятельности студентов по овладению программным материалом учебной дисциплины.

Порядок подготовки лекционного занятия включает в себя выполнение следующих этапов:

- изучение требований программы дисциплины;
- определение целей и задач лекции;
- разработка плана проведения лекции;
- подбор литературы (ознакомление с методической литературой, публикациями периодической печати по теме лекционного занятия);
- отбор необходимого и достаточного по содержанию учебного материала;
- определение методов, приемов и средств поддержания интереса, внимания, стимулирования творческого мышления студентов;
- написание конспекта лекции.

Лекция должна включать следующие разделы:

- формулировку темы лекции;
- указание основных изучаемых разделов или вопросов и предполагаемых затрат времени на их изложение;
- изложение вводной части;
- изложение основной части лекции;
- краткие выводы по каждому из вопросов;
- заключение;
- рекомендации литературных источников по излагаемым вопросам.

Лабораторные занятия

Лабораторное занятие − целенаправленная форма организации педагогического процесса, направленная на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Они развивают научное мышление и речь, позволяют проверить знания студентов и выступают как средства оперативной обратной связи.

Правильно организованные лабораторные занятия ориентированы на решение следующих задач:

- обобщение, систематизация, углубление, закрепление полученных на лекциях и в процессе самостоятельной работы теоретических знаний по дисциплине (предмету);
- формирование практических умений и навыков, необходимых в будущей профессиональной деятельности, реализация единства интеллектуальной и практической деятельности;
- выработка при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Состав заданий для лабораторного занятия должен быть спланирован с расчетом, чтобы за отведенное время они могли быть качественно выполнены большинством учащихся.

Лабораторные занятия должны так быть организованы, чтобы студенты ощущали нарастание сложности выполнения заданий, испытывали бы положительные эмоции от переживания собственного успеха в учении, поисками правильных и точных решений.

Самостоятельная работа

Самостоятельная работа – это вид учебной деятельности, которую студент совершает в установленное время и в установленном объеме индивидуально или в группе, без непосредственной помощи преподавателя (но при его контроле), руководствуясь сформированными ранее представлениями о порядке и правильности выполнения действий.

В учебном процессе образовательного учреждения выделяются два вида самостоятельной работы:

- аудиторная – выполняется на учебных занятиях, под непосредственным руководством преподавателя и по его заданию (выполнение самостоятельных работ; выполнение контрольных и практических работ; решение задач);
- внеаудиторная – выполняется по заданию преподавателя, но без его непосредственного участия (подготовка к аудиторным занятиям; изучение учебного материала, вынесенного на самостоятельную проработку; выполнение домашних заданий разнообразного характера; выполнение индивидуальных заданий, направленных на развитие у студентов самостоятельности и инициативы; подготовка к контрольной работе). Внеаудиторные самостоятельные работы представляют собой логическое продолжение аудиторных занятий, проводятся по заданию преподавателя, который инструктирует студентов и устанавливает сроки выполнения задания.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Лекция

- Лекция – основной вид обучения в вузе.
- В лекции излагаются основные положения теории, ее понятия и законы, приводятся факты, показывающие связь теории с практикой.
- Накануне лекции необходимо повторить содержание предыдущей лекции (а также теорию по изучаемой теме в школьных учебниках геометрии, если эта тема была представлена в них), а затем посмотреть тему очередной лекции по программе (по плану лекций).
- Полезно вести записи (конспекты) лекций: для непонятных вопросов оставлять место при работе над темой лекции с учебными пособиями.
- Записи лекций следует вести в отдельной тетради, оставляя место для дополнений во время самостоятельной работы.
- При конспектировании лекций выделяйте главы и разделы, параграфы, подчеркивайте основное.

Лабораторное занятие

- Лабораторное занятие – наиболее активный вид учебных занятий в вузе. Он предполагает самостоятельную работу над лекциями и учебными пособиями.
- К каждому лабораторному занятию нужно готовиться. Подготовку следует начинать с повторения теории (по записям лекций или по учебному пособию). После этого нужно решать задачи из предложенного домашнего задания.

Организация самостоятельной работы

Самостоятельность в учебной работе способствует развитию заинтересованности студента в изучаемом материале, вырабатывает у него умение и потребность самостоятельно получать знания, что весьма важно для специалиста с высшим образованием. Самостоятельная работа студентов представлена в следующих формах:

- работа с учебной литературой и конспектом лекций с целью подготовки к лабораторным занятиям, составление конспектов тем, выносимых на самостоятельную проработку;
- систематическое выполнение домашних работ.

Таблица 4 – Содержание самостоятельной работы обучающихся

Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
Раздел 1. Линейные коды	30	Подготовка отчета по лабораторной работе №1
Раздел 2. БЧХ/РС коды	30	Подготовка отчета по лабораторной работе №2
Раздел 3. Сверточные коды	30	Подготовка отчета по лабораторной работе №3

Раздел 4. Коды с малой плотностью проверок на четность	30	Подготовка отчета по лабораторной работе №4

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины (модуля), выполняемые обучающимися самостоятельно

Лабораторная работа 1

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.

Лабораторные работы должны быть сданы в период прочтения курса.

Сдача работы представляет собой предоставление отчета в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

Лабораторная работа 2

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.

Лабораторные работы должны быть сданы в период прочтения курса.

Сдача работы представляет собой предоставление отчета в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

Лабораторная работа 3

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.

Лабораторные работы должны быть сданы в период прочтения курса.

Сдача работы представляет собой предоставление отчета в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

Лабораторная работа 4

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.

Лабораторные работы должны быть сданы в период прочтения курса.

Сдача работы представляет собой предоставление отчета в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине «Теория кодирования» могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line или off-line в формах.

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Линейные коды	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабора-*

			торной работы
БЧХ/РС коды	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторной работы*
Сверточные коды	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторной работы*
Коды с малой плотностью проверок на четность	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторной работы*

6.2. Информационные технологии

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

- система управления обучением LMS Moodle;
- использование возможностей Интернета в учебном процессе (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т.д.);
- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источник информации;
- использование возможностей электронной почты;
- использование средств представления учебной информации (электронных учебных пособий, применение новых технологий для проведения занятий с использованием презентаций и т.д.);
- использование интерактивных средств взаимодействия участников образовательного процесса (технологии дистанционного или открытого обучения в глобальной сети);
- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс).

6.3. Современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Пакет офисных программ
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Google Chrome	Браузер
OpenOffice	Пакет офисных программ

6.3.2. Современные профессиональные базы данных и информационные справоч-ные системы

1. Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех». https://biblio.asu.edu.ru
2. Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента». www.studentlibrary.ru.
3. Электронная библиотечная система издательства ЮРАЙТ, раздел «Легендарные книги». www.biblio-online.ru
4. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информсистем». https://library.asu.edu.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине «Теория кодирования» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин и прохождением практик, а в процессе освоения дисциплины– последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины, результатов обучения по дисциплине и оценочных средств

№ п/п	Контролируемые разделы, темы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1	Линейные коды	ПК-3, ПК-8	Лабораторная работа №1
2	БЧХ/РС коды	ПК-3, ПК-8	Лабораторная работа №2
3	Сверточные коды	ПК-3, ПК-8	Лабораторная работа №3
4	Коды с малой плотностью проверок на четность	ПК-3, ПК-8	Лабораторная работа №4

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов

Шкала оценивания	Критерии оценивания
2 «неудовлетворительно»	не способен правильно выполнить задания

7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Лабораторная работа 1

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.
Лабораторные работы должны быть сданы в период прочтения курса.
Сдача работы представляет собой предоставление отчета в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

Примеры заданий к лабораторной работе 1 «Линейные коды»

1. Студенты должны выполнить декодирование в канале с мягкими и жесткими решениями с помощью декодера Витерби.
2. Студенты должны найти спектр кода и построить график зависимости оценки вероятности ошибки декодирования в гауссовском канале и ДСК.
3. Студенты должны знать основные определения теории линейных кодов.
4. Студенты должны обладать способностью анализировать коды с помощью границ Варшамова-Гилберта и Хэмминга.
5. Студенты должны обладать способностью анализировать коды с помощью границ Плоткина и Грайсмера.
6. Студенты должны уметь кодировать и декодировать информацию с применением линейных кодов.
7. Студенты должны уметь оценивать вероятность ошибки декодирования.

Порядок предоставления отчета по лабораторной работе

Отчет по лабораторной работе представляется в печатном виде в формате, предусмотренном шаблоном отчета по лабораторной работе. Время, отводимое на выполнение – 4 часа. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Шаблон отчета по лабораторной работе

Отчет по лабораторной работе № ____
«*Название лабораторной работы*»
1. Цель и задачи лабораторной работы: ____
2. Методика проведения исследования: ____
3. Анализ погрешностей: ____
4. Результаты: ____
5. Выводы: ____

Требования к выполнению лабораторной работы

Отчеты по лабораторным работам должны быть отправлены на электронную почту преподавателя не позднее, чем через две недели после выдачи задания. Полученные выводы и графический материал должны быть информативными и корректными.

Лабораторная работа 2

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.
Лабораторные работы должны быть сданы в период прочтения курса.

Сдача работы представляет собой предоставление отчета в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

Примеры заданий к лабораторной работе 2 «БЧХ/РС коды»

1. Студенты должны найти минимальный многочлен для корней и построить порождающий многочлен кода.
2. Студенты должны выполнить все этапы декодирования и найти ошибочные позиции.
3. Студенты должны знать основные понятия теории циклических и БЧХ/РС кодов.
4. Студенты должны знать основные понятия теории каскадных кодов.
5. Студенты должны уметь оценивать асимптотические границы на расстояния различных кодов.

Порядок предоставления отчета по лабораторной работе

Отчет по лабораторной работе представляется в печатном виде в формате, предусмотренном шаблоном отчета по лабораторной работе. Время, отводимое на выполнение – 4 часа. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Шаблон отчета по лабораторной работе

Отчет по лабораторной работе № ____

«*Название лабораторной работы*»

1. Цель и задачи лабораторной работы: ____
2. Методика проведения исследования: ____
3. Анализ погрешностей: ____
4. Результаты: ____
5. Выводы: ____

Требования к выполнению лабораторной работы

Отчеты по лабораторным работам должны быть отправлены на электронную почту преподавателя не позднее, чем через две недели после выдачи задания. Полученные выводы и графический материал должны быть информативными и корректными.

Лабораторная работа 3

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.

Лабораторные работы должны быть сданы в период прочтения курса.

Сдача работы представляет собой предоставление отчета в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

Примеры заданий к лабораторной работе 3 «Сверточные коды»

1. Для заданного сверточного кода постоить решетчатую диаграмму.
2. Найти свободное расстояние и первые 5 коэффициентов спектров.
3. Построить зависимость оценок вероятности ошибочного события и вероятности ошибки на бит как функцию отношения сигнал/шум на бит.
4. Студенты должны знать основные понятия теории сверточных кодов.
5. Стдуенты должны уметь строить решетчатые диаграммы сверточных кодов.
6. Студенты должны оценивать вероятность ошибочного события при сверточном декодировании.
7. Студенты должны использовать комбинирование кодов для достижения высокой эффективности кодирования.

Порядок предоставления отчета по лабораторной работе

Отчет по лабораторной работе представляется в печатном виде в формате, предусмотренном шаблоном отчета по лабораторной работе. Время, отводимое на выполнение – 4 часа. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Шаблон отчета по лабораторной работе

Отчет по лабораторной работе № ____

«*Название лабораторной работы*»

1. Цель и задачи лабораторной работы: ____
2. Методика проведения исследования: ____
3. Анализ погрешностей: ____
4. Результаты: ____
5. Выводы: ____

Требования к выполнению лабораторной работы

Отчеты по лабораторным работам должны быть отправлены на электронную почту преподавателя не позднее, чем через две недели после выдачи задания. Полученные выводы и графический материал должны быть информативными и корректными.

Лабораторная работа 4

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.

Лабораторные работы должны быть сданы в период прочтения курса.

Сдача работы представляет собой предоставление отчета в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

Примеры заданий к лабораторной работе 3 «Сверточные коды»

1. Для заданного сверточного кода построить решетчатую диаграмму.
2. Найти свободное расстояние и первые 5 коэффициентов спектров.
3. Построить зависимость оценок вероятности ошибочного события и вероятности ошибки на бит как функцию отношения сигнал/шум на бит.
4. Студенты должны знать основные понятия теории сверточных кодов.
5. Стдуенты должны уметь строить решетчатые диаграммы сверточных кодов.
6. Студенты должны оценивать вероятность ошибочного события при сверточном декодировании.
7. Студенты должны использовать комбинирование кодов для достижения высокой эффективности кодирования.

Порядок предоставления отчета по лабораторной работе

Отчет по лабораторной работе представляется в печатном виде в формате, предусмотренном шаблоном отчета по лабораторной работе. Время, отводимое на выполнение – 4 часа. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Шаблон отчета по лабораторной работе

Отчет по лабораторной работе № ____

«*Название лабораторной работы*»

1. Цель и задачи лабораторной работы: ____
2. Методика проведения исследования: ____
3. Анализ погрешностей: ____
4. Результаты: ____
5. Выводы: ____

Требования к выполнению лабораторной работы

Отчеты по лабораторным работам должны быть отправлены на электронную почту преподавателя не позднее, чем через две недели после выдачи задания. Полученные выводы и графический материал должны быть информативными и корректными.

Перечень вопросов и заданий, выносимых на экзамен

1. Конфиденциальность, целостность, доступность информации. Классификация атак. Классификация угроз.

2. Экспоненциальная сложность. Полиномиальная сложность.
3. О-нотация
4. Кольцо, определение.
5. Группа, определение.
6. Поля Галуа.
7. Кольцо вычетов. Доказать, что множество Zn является кольцом.
8. Мультипликативная группа. Доказать, что множество Zn* является мультипликативной группой.
9. Наибольший общий делитель.
10. Алгоритм Евклида.
11. Расширенный алгоритм Евклида.
12. Функция Эйлера. Теорема Эйлера.
13. Китайская теорема об остатках.
14. Двоичный код.
15. Расстояние Хэмминга.
16. Кодовое расстояние.
17. Линейный код.
18. Порождающая и проверочная матрицы линейного кода.
19. Код Хэмминга и его свойства.
20. Определение циклического кода, свойства.
21. Архитектура кодера и декодера для цилического кода.
22. Код Боуза-Чоудхури-Хоквингема.
23. Мажоритарное декодирование линейных кодов.
24. Коды Рида-Маллера, их свойства.
25. Недвоичные циклические коды.
26. Код Рида-Соломона, его свойства.
27. Шифр сдвига.
28. Шифр замены.
29. Шифр Виженера.
30. Перестановочные шифры.
31. Одноразовый шифр-блокнот.
32. Теоретико-информационная стойкость. Энтропия.
33. Алгоритм шифрования AES.
34. Алгоритм шифрования 3DES.
35. Алгоритм шифрования RC4.
36. Задача факторизации.
37. Задача дискретного логарифмирования.
38. Протокол широкоротой лягушки.
39. Протокол Нидхейма-Шредера.
40. Протокол Отвэй-Риса.
41. Алгоритм шифрования RSA.
42. Эффективная реализация расшифрования RSA.
43. Атака на RSA: разделенный модуль.
44. Атака на RSA: малая шифрующая экспонента.
45. Атака на RSA: метод факторизации Ферма.
46. Схемы разделение секрета.
47. Алгоритм DSA.
48. Подпись Шнорра.
49. Подпись Ниберга-Руппеля.
50. Протокол электронного голосования.

Порядок формирования экзаменационного билета:

Билеты состоят из 2-х вопросов:

1 вопрос – с 1 по 25 вопрос из перечня вопросов к экзамену;
2 вопрос – с 26 по 50 вопрос из перечня вопросов к экзамену.
Пример экзаменационного билета № 1
1. Порождающая и проверочная матрицы линейного кода.
2. Алгоритм шифрования RSA.

Таблица 9. Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-3. Способен обеспечивать заданный уровень производительности, надежности и безопасности при создании вариантов архитектуры программного средства.				
1.	Задание закрытого типа	*Выберите правильный вариант ответа.* Код – это... а. Случайный набор символов, с помощью которых представлена информация б. Система условных знаков для представления информации в. Буквенные символы, представленные цифровыми значениями г. Цифровые значения, представленные буквенными символами	а	1-3
2.		*Выберите правильный вариант ответа.* Средствами кодирования информации НЕ может выступать: а. сигнал б. знак в. буква г. свойство д. звук	г	1-3
3.		*Выберите правильный вариант ответа.*	а	1-3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		Кодирование – это.. а. преобразование обычного, понятного текста в код б. написание программы в. совокупность способов структурирования данных		
4.		*Выберите правильный вариант ответа.* Как осуществляется дешифрование текста при аналитических преобразованиях? а. умножение матрицы на вектор б. деление матрицы на вектор в. перемножение матриц	а	1-3
5.		*Выберите правильный вариант ответа.* Из скольки последовательностей состоит расшифровка текста по таблице Вижинера? а. 3 б. 4 в. 5	а	1-3
6.	Задание открытого типа	Сформулируйте основную идею метода перестановки.	Суть метода перестановки заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов.	2-5
7.		Какие таблицы Вижинера можно использовать для повышения стойкости шифрования?	1. Во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке. 2. В качестве ключа используется случай-	2-5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			ность последовательных чисел.	
8.		Сформулируйте основную идею алгоритма гаммирования.	Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле.	
9.		Что понимают под *виртуальным контейнером?*	Зашифрованный файл, хранящийся на логическом диске, который подключается к системе как еще один логический диск.	2-5
10.		Опишите суть протокола Нидхема-Шрёдера.	Нидхема — Шрёдера — общее название для симметричного и асимметричного протоколов аутентификации и обмена ключами. Оба протокола были предложены Майклом Шрёдером и Роджером Нидхемом[1]. Вариант, основанный на симметричном шифровании, использует промежуточную доверенную сторону. Этот протокол стал основой для целого класса подобных протоколов. Например, Kerberos является одним из вариантов симметричного протокола Нидхема — Шрёдера. Вариант, основанный на асимметричном шифровании, предназначен для взаимной аутентификации сторон. В оригинальном виде оба варианта протокола являются уязвимыми	5-8
11.	Задание комбинированного типа	Верно ли утверждение: В шифре ГОСТ используется 246-битовый ключ. Поясните ответ.	Нет, утверждение неверно, поскольку в шифре ГОСТ используется 256-битовый ключ.	1-3
	ПК-8. Способность понимать, совершенствовать и применять современный математический аппарат.			
	1	Задание закрытого типа	*Выберите правильный вариант ответа.* Что может использоваться в качестве гаммы при гаммировании? а. любая последовательность случайных символов	а	1-3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		б. любая последовательность чисел в. любая последовательность букв г. любая последовательность чисел и букв		
	1	*Выберите правильный вариант ответа.* Ключ алгоритма ГОСТ – это... а. массив, состоящий из 32-мерных векторов б. последовательность чисел в. алфавит	а	1-3
	1	*Выберите правильный вариант ответа.* Блок управления – это... а. набор регистров, сумматоров, блоков подстановки, связанных между собой шинами передачи данных б. файлы, использующие различные методы кэширования в. язык описания данных	а	1-3
	1	*Выберите правильный вариант ответа.* Устройство, дающее статически случайныый шум – это... а. генераторы случайных чисел б. контроль ввода данных на	а	1-3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		компьютер в. УКЗХ		
1		*Выберите правильный вариант ответа.* Сколько существуют перестановок в стандарте DES? а. 2 б. 3 в. 4	б	1-3
1	Задание открытого типа	Что такое коды Боуза-Чоудхури-Хоквингема?	Коды Боуза — Чоудхури — Хоквингема, сокращённо БЧХ-коды — в теории кодирования это широкий класс циклических кодов, применяемых для защиты информации от ошибок. Отличается возможностью построения кода с заранее определёнными корректирующими свойствами, а именно, минимальным кодовым расстоянием. Частным случаем БЧХ-кодов является код Рида — Соломона. Код был разработан Алексисом Хоквингемом в 1959 году и независимо от него Раджем Чандра Боузом и Дидженом Рэй-Чоудхури в 1960 году.	5-8
1		Сформулируйте задачу дискретного логарифмирования.	Пусть в некоторой конечной мультипликативной абелевой группе G задано уравнение $g^x = a$. Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x, удовлетворяющего уравнению. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы. Это сразу даёт грубую оценку сложности алгоритма поиска решений сверху — алгоритм полного перебора нашёл бы решение за число шагов не выше порядка данной группы.	2-5
1		Решите задачу дискретного логарифмирования в кольце вычетов по модулю простого числа. Пусть задано сравнение	Выпишем таблицу всех степеней числа 3. Каждый раз мы вычисляем остаток от деления на 17 (например, $3^3 \equiv 27$ — остаток от деления на 17 равен 10).	8-10

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		$3^x \equiv 13\ (mod\ 17)$ методом перебора.	$3^1 \equiv 3$ $3^2 \equiv 9$ $3^3 \equiv 10$ $3^4 \equiv 13$ $3^5 \equiv 5$ $3^6 \equiv 15$ $3^7 \equiv 11$ $3^8 \equiv 16$ $3^9 \equiv 14$ $3^{10} \equiv 8$ $3^{11} \equiv 7$ $3^{12} \equiv 4$ $3^{13} \equiv 12$ $3^{14} \equiv 2$ $3^{15} \equiv 6$ $3^{16} \equiv 1$ Теперь легко увидеть, что решением рассматриваемого сравнения является $x = 4$, поскольку $3^4 \equiv 13$.	
	2(	Для чего используется схема Шнорра?	Схема Шнорра (англ. schnorr scheme) — одна из наиболее эффективных и теоретически обоснованных схем аутентификации. Безопасность схемы основывается на трудности вычисления дискретных логарифмов. Предложенная Клаусом Шнорром[англ.] схема является модификацией схем Эль-Гамаля (1985) и Фиата-Шамира (1986), но имеет меньший размер подписи. Схема Шнорра лежит в основе стандарта Республики Беларусь СТБ 1176.2-99 и южнокорейских стандартов KCDSA и EC-KCDSA. Она была покрыта патентом США 4999082, который истек в феврале 2008 года.	5-8
	2	Дайте определение протоколу тайного голосования.	В криптографии протоколы тайного голосования — протоколы обмена данными для реализации безопасного тайного электронного голосования через интернет при помощи компьютеров, телефонов или других специальных вычислительных машин. Это направление криптографии всё ещё развивается, но уже применяется на практике. Многие страны мира уже внедряют электронные голосования на муниципальном уровне и выше. Для уверенности в правильности, надёжности и конфиденциальности таких выборов и используют протоколы с доказанной защищённостью, которые опираются на проверенные криптографические системы, вроде асимметричного шифрования и электронной подписи. Кроме того, им нужна готовая материальная и юридическая база. Слияние всех этих факторов образует непосредственный инструмент электронной демократии.	5-8

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Таблица 10. Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторных работ*	4/10	40	Сроки указаны в Moodle
Всего			**40**	-
Блок бонусов				
2.	*Посещение занятий*		10	
Всего			**10**	-
Дополнительный блок**				
3.	*Экзамен*		50	
Всего			**50**	-
ИТОГО			**100**	-

Таблица 11. Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине

Сумма баллов	Оценка по 4-балльной шкале
90–100	5 (отлично)
85–89	4 (хорошо)
75–84	
70–74	
65–69	3 (удовлетворительно)
60–64	
Ниже 60	2 (неудовлетворительно)

При реализации дисциплины в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Hopcroft J. E., Motwani R., Ullman J. D. Introduction to Automata Theory, Languages, and Computation (3rd Edition). — Addison-Wesley, Boston, MA, USA, 2006. — 750 с.
2. Шень А. Программирование: теоремы и задачи. — М.: МЦНМО, 2014. — 296 с.
3. Шень А., Верещагин Н. Языки и исчисления. — М.: МЦНМО, 2012. — 240 с.
4. Верещагин, Н. К. Колмогоровская сложность и алгоритмическая случайность [Электронный ресурс] / Н. К. Верещагин, В. А. Успенский, А. Шень. — Электрон. дан. — СПб: Лань, 2013. — 575 с. — Режим доступа: https://e.lanbook.com/book/56395 — Загл. с экрана.
5. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов - 2-е изд. / А. Б. Лось,А. Ю. Нестеренко,М. И. Рожков.. Москва : Юрайт, 2022. - 473с. - Текст: электронный. - URL: https://urait.ru/bcode/489242

8.2. Дополнительная литература

1. Кривцова, И. Е. Основы дискретной математики. Часть 1. Учебное пособие [Электронный ресурс] / И. Е. Кривцова, И. С. Лебедев, А. В. Настека. — Электрон. дан. — СПб: ИТМО, 2016. — 92 с. — Режим доступа: http://books.ifmo.ru/book/1869/osnovy_diskretnoy_matematiki._chast_1._uchebnoe_posobie.htm — Загл. с экрана.
2. Теория информации и кодирования : учебное пособие / М. Ю. Конышев, П. Ю. Пушкин, Ю. А. Лежнина [и др.] ; под редакцией М. Ю. Конышева. — Москва : РТУ МИРЭА, 2024. — 308 с. — ISBN 978-5-7339-2232-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/421145

8.3. Интернет-ресурсы, необходимые для освоения дисциплины

1. Вики-конспекты. — http://neerc.ifmo.ru/wiki/index.php?title=Заглавная_страница
2. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-

систем»: https://library.asu.edu.ru

3. Корпоративный проект Ассоциации региональных библиотечных консорциумов (АРБИКОН) «Межрегиональная аналитическая роспись статей» (МАРС): http://mars.arbicon.ru

4. Единое окно доступа к образовательным ресурсам http://window.edu.ru

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для проведения **лекционных занятий**:

1. Используется аудитория, оборудованная необходимым количеством столов, стульев, доской маркерной и электронной.
2. Аудитория должна иметь следующие нормы освещенности
   - СНиП 23-05-95 «Естественное и искусственное освещение» норма освещенности аудиторий ВУЗов 400 Лк.
   - СанПиН 2.2.1/2.1.1.1278-03 «Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий» пункт 3.3.3. «Общее освещение в помещениях общественных зданий должно быть равномерным».
3. Электронная доска должна быть подключена к сети Интернет.

Для проведения **лабораторных занятий**:

1. Лабораторные занятия проводятся с группами или подгруппами не более 15 человек.
2. Аудитория должна быть оснащена необходимым количеством столов, стульев, доской маркерной и электронной.
4. Аудитория должна иметь следующие нормы освещенности
   - СНиП 23-05-95 «Естественное и искусственное освещение» норма освещенности аудиторий ВУЗов 400 Лк.
   - СанПиН 2.2.1/2.1.1.1278-03 «Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий» пункт 3.3.3. «Общее освещение в помещениях общественных зданий должно быть равномерным».
5. В аудитории должно быть не менее 15 компьютеров, находящихся в исправном состоянии.
6. Расположение компьютеров в аудитории должно позволять преподавателю подойти к рабочему месту студента.
7. Компьютеры должны быть соединены локальной сетью со скоростью не менее 1 Гбит/с и подключены к сети Интернет.
8. Компьютеры должны обладать минимальными характеристиками:
   - Объем оперативной памяти 16 Гб
   - Накопитель SDD 500 Гб
   - Процессор 12th Gen Intel(R) Core(TM) i3-12100
   - Видеоадаптер Intel(R) UHD Graphics 730

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).