Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
_____ М.М. Лаврентьев
«03» июля 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Введение в теорию кодирования

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Программная инженерия и компьютерные науки

Форма обучения: очная
Год обучения:3, семестр: 6

№	Вид деятельности	Семестр
		6
1	Лекции, час.	32
2	Практические занятия, час.	32
3	Лабораторные занятия, час.	
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	66
5	в электронной форме, час.	
6	из них аудиторных занятий, час.	64
7	из них в активной и интерактивной форме, час.	24
8	консультаций, час.	2
9	Самостоятельная работа, час.	76
10	в том числе на выполнение письменных работ, час	
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	Э 2
12	Всего зачетных единиц[1]	4

Новосибирск 2019

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования - магистратура по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки от 19.09.2017 № 929.

Место дисциплины в структуре учебного плана: Блок 1 Дисциплины (модули), обязательная часть, обязательная дисциплина.

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 02.07.2019, протокол № 75.

Программу разработал:

Доцент кафедры дискретного анализа и исследований операций ФИТ,
кандидат физико-математических наук И. Ю. Могильных

Заведующий кафедрой дискретного анализа и исследований операций ФИТ,
доктор физико-математических наук В. Л. Береснев

Ответственный за образовательную программу:
доцент кафедры систем информатики ФИТ,
кандидат технических наук А. А. Романенко

Аннотация к рабочей программе дисциплины
«Введение в теорию кодирования»

Дисциплина «**Введение в теорию кодирования**» реализуется в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): ПРОГРАММНАЯ ИНЖЕНЕРИЯ И КОМПЬЮТЕРНЫЕ НАУКИ, по очной форме обучения на русском языке.

Место в образовательной программе: Дисциплина «Введение в теорию кодирования» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения ряда базовых областей математики: «Дискретная математика», «Алгебра и геометрия», «Теория вероятностей и математическая статистика», «Математическая логика и теория алгоритмов». Кроме того, повышению понимания предмета «Введение в теорию кодирования» способствуют наличие общих навыков работы с компьютером как средством управления информацией, а также наличие знаний в сфере устройства и функционирования глобальных компьютерных сетей.

Дисциплина «Введение в теорию кодирования» реализуется в 6 семестре в рамках обязательной части дисциплин (модулей) Блока 1 и является обязательной дисциплиной.

Дисциплина «Введение в теорию кодирования» направлена на формирование компетенций:

Способен разрабатывать алгоритмы и программы, пригодные для практического применения (ОПК-8), в части следующих индикаторов достижения компетенции:

ОПК-8.1 Знать: алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения

Перечень основных разделов дисциплины: Дисциплина «Введение в теорию кодирования» предполагает ознакомление с основными понятиями и теоретическими основами теории защиты информации — методов передачи, хранения и защиты информации по различным каналам связи, а именно:

— теории кодов, исправляющих ошибки в каналах связи с шумами;

— криптологии, состоящей из криптографии и криптоанализа;

— сжатия данных (передачи информации по каналам связи без шума).

Основной целью освоения дисциплины является обучение студентов основам математических знаний по части алгебраической и комбинаторной теории кодов, исправляющих ошибки, криптологии и сжатия данных, а также получение высшего профессионального образования, позволяющего выпускнику успешно проводить ориентированные на производство разработки и научные исследования, направленные на развитие и применение информационных технологий.

В части курса, посвященной теории кодирования, предлагается ознакомление с базовыми понятиями теории линейных кодов, а также теории циклических кодов. Эти классы кодов наиболее часто применяются на практике. Теория кодирования самым тесным образом связана с дискретным анализом, теорией групп, теорией Галуа, конечными геометриями, теорией графов, теорией блок-схем (design theory), криптографией.

Вторая часть курса посвящена введению в криптологию, здесь излагаются основные стандарты шифрования данных (DES, AES, российский стандарт шифрования данных ГОСТ Р 34.12-2015), теорема Шеннона о существовании совершенно секретных шифров, а

также основные криптосистемы с открытыми ключами: криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма, криптосистема Шамира, криптосистема, основанная на эллиптических кривых, цифровые подписи, базирующиеся на основных криптосистемах.

В третьей части курса, посвященной сжатию данных излагаются основные методы сжатия данных — методы побуквенного кодирования (коды Фано, Хаффмена, Шеннона), критерий однозначности кодирования, теорема Шеннона; основные методы адаптивного кодирования (методы Лемпела — Зива, код «стопка книг», арифметический код).

В процессе преподавания дисциплины «Введение в теорию кодирования» применяются следующие образовательные технологии:

— проведение лекционных и практических занятий;
— консультации;
— индивидуальная и коллективная работа.

При освоении дисциплины студенты выполняют следующие виды учебной работы: лекций, практические занятия, консультации, самостоятельная работа. В учебном процессе предусматривается использование активных и интерактивных форм проведения занятий. В том числе, предполагаются такие формы, как решение задач у доски перед аудиторией с обоснованием способа решения, участие в дискуссиях об эффективности того или иного метода.

Самостоятельная работа включает: подготовку к практическим занятиям по разделам дисциплины, выполнение еженедельного домашнего задания, подготовку к письменной контрольной работе, подготовку к коллоквиумам и экзамену.

Общий объем дисциплины – 4 зачетных единиц (144 часа).

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Введение в теорию кодирования» осуществляется в форме сдачи коллоквиумов по основным разделам дисциплины, в рамках которых студенты показывают свои теоретические знания в устной беседе с преподавателем. Результаты сдачи коллоквиумов оцениваются по шкале «неудовлетворительно», «удовлетворительно», «хорошо», «отлично» и составляют одно из условий успешного прохождения промежуточной аттестации.

Промежуточная аттестация по дисциплине «Введение в теорию кодирования» проводится по завершению периода ее освоения (семестра) и состоит из устного экзамена.

Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Учебно-методическое обеспечение дисциплины.

Учебно-методический комплекс по дисциплине «Введение в теорию кодирования» в электронной информационно-образовательной среде НГУ: http://codingtheory.nsu.ru

Другие пособия и методические работы:

- Соловьева Ф. И. Введение в теорию кодирования: Учеб. пособие 2-е изд. / Новосиб. гос. ун-т. Новосибирск, 2011. 124 с. Режим доступа: [http://tc.nsu.ru/uploads/codingtheory.pdf]

- Соловьева Ф. И, Лось А. В., Могильных И. Ю. Сборник задач по теории кодирования, криптологии и сжатию данных: учебное пособие [для студентов Мех-мат. фак. и Фак. информ. технологий НГУ] / М-во образования и науки РФ, Новосиб. нац. исслед. гос. ун-т, Фак. информ. технологий — Новосибирск: Редакционно-издательский центр НГУ, 2013 . 99 с. Режим доступа: [http://e-lib.nsu.ru/dsweb/Get/Resource-895/page001.pdf].

1. Внешние требования к дисциплине

Таблица 1.1

Компетенция ОПК-8. Способен разрабатывать алгоритмы и программы, пригодные для практического применения, *в части следующих индикаторов достижения компетенции:*
ОПК-8.1 Знать: алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения

1. Требования к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**		
	Лекции	**Практики / семинары**	**Самостоятельная работа**
ОПК-8.1 Знать: алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения			
1. Знать основные понятия и теоретические основы теории защиты информации	+	+	+
2. Иметь представление о существующих методах обеспечения информационной безопасности компьютерных систем	+	+	+
3. Уметь применять математические методы для решения практических задач в области передачи, хранения и обработки информации		+	+

2. Содержание и структура учебной дисциплины

Темы лекций	**Активные формы, час. (входит в общее кол-во часов)**	**Часы**	**Ссылки на результаты обучения**
Семестр: 6			
1. Теория кодирования			
1.1. Модель канала связи, скорость кода, пропускная способность. Теорема Шеннона (без доказательства). Вероятность ошибки декодирования. Стандартное расположение. Синдром	0	2	1, 2
1.2. Поле Галуа, его свойства, примеры полей Галуа	0	2	1
1.3. Линейные коды. Кодирование и декодирование. Общие свойства линейных кодов. Теорема о связи проверочной и порождающей матриц	0	2	1, 2
1.4. Теорема Глаголева	0	1	1
1.5. Границы объема кода: граница Синглтона, граница Хэмминга, граница Варшамова-Гилберта. Методы построения новых кодов из заданных. Комбинирование кодов. Теорема Плоткина. Каскадная конструкция.	0	3	1, 2
1.6. Совершенные коды. Теорема о существовании	0	2	1, 2

совершенных кодов. Коды Хэмминга над GF(q), способы задания, кодирование, декодирование, единственность. Конструкция кодов Васильева. Оценки снизу и сверху числа совершенных кодов.			
1.7. Циклические коды. Кольцо многочленов над полем Галуа. Определение циклического кода. Теорема о необходимом и достаточном условии существования циклического кода с порождающим многочленом g(x). Кодирование и декодирование циклических кодов.	0	2	1, 2
1.8. Примеры циклических кодов: коды Хэмминга, коды Боуза — Чоудхури — Хоквингема (БЧХ-коды), коды Рида — Соломона.	0	2	2
2. Сжатие информации			
2.1. Разделимые и префиксные коды. Стоимость кодирования. Неравенство Крафта — Макмиллана. Теорема Крафта. Теорема Макмиллана.	0	2	1, 2
2.2. Оптимальное кодирование. Метод Хаффмана. Метод Фано.	0	0,5	1, 2
2.3. Метод Шеннона для бернуллиевских источников. Энтропия. Теорема Шеннона	0	1,5	1, 2
2.4. Критерий разделимости побуквенного кодирования. Теоремы Маркова. Алгоритм распознавания разделимости кода.	0	2	1
2.5. Универсальное кодирование, теорема Фитингофа	0	0,5	1, 2
2.6. Код Левенштейна. Адаптивные методы сжатия данных. Код «стопка книг». Методы Лемпела — Зива и их модификации. Адаптивный метод Хаффмана. Арифметический код.	0	1,5	1, 2
3. Элементы криптологии			
3.1. Введение в криптологию. Секретность и имитостойкость. Криптография и криптоанализ.	0	0,5	1, 2
3.2. Криптографические системы с секретными ключами. Полиалфавитные шифры. Шифр с бегущим ключом	0	0,5	1, 2
3.3. Теорема Шеннона о существовании совершенно секретных шифров	0	1	1, 2
3.4. Стандарт шифрования данных (криптосистема AES, криптосистема ГОСТ, криптосистема DES).	0	0,5	1, 2
3.5. Криптографические системы с открытыми ключами. Односторонняя функция с лазейкой. «Шарады» Меркля	0	0,5	1, 2
3.6. Криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма. Криптосистема Эль-Гамаля. Криптосистема Шамира	0	1,5	1, 2
3.7. Криптосистема RSA и проблема разложения числа на простые сомножители	0	0,5	1, 2
3.8. Цифровая подпись	0	0,25	1, 2
3.9. Криптосистема Меркля — Хэллмана, основанная на задаче об укладке ранца	0	0,75	1, 2
3.10. Кодирующие системы Мак-Эллиса и Нидеррайтера	0	1	1, 2
3.11. Криптография на эллиптических кривых	0	1	1, 2
Итого:		**32**	

Таблица 3.2

Темы практических занятий	Активные формы, час. (входит в общее кол-во часов)	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 6				
Раздел 1 «Теория кодирования»				
Модель канала связи, скорость кода, пропускная способность. Теорема Шеннона (без доказательства). Вероятность ошибки декодирования. Стандартное расположение. Синдром	1	2	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Поле Галуа, его свойства, примеры полей Галуа	1	2	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Линейные коды. Кодирование и декодирование. Общие свойства линейных кодов. Теорема о связи проверочной и порождающей матриц	1	2	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Теорема Глаголева	0,5	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Границы объема кода: граница Синглтона, граница Хэмминга, граница Варшамова — Гилберта. Методы построения новых кодов из заданных. Комбинирование кодов. Теорема Плоткина. Каскадная конструкция	1,5	3	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Совершенные коды. Теорема о существовании совершенных кодов. Коды Хэмминга над GF(q), способы задания, кодирование, декодирование, единственность. Конструкция кодов Васильева. Оценки снизу и сверху числа	1	2	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий

совершенных кодов				
Циклические коды. Кольцо многочленов над полем Галуа. Определение циклического кода. Теорема о необходимом и достаточном условии существования циклического кода с порождающим многочленом g(x). Кодирование и декодирование циклических кодов	1,5	3	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Примеры циклических кодов: коды Хэмминга, коды Боуза — Чоудхури — Хоквингема (БЧХ-коды), коды Рида — Соломона	0,5	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Раздел 2 «Сжатие данных»				
Разделимые и префиксные коды. Стоимость кодирования. Неравенство Крафта — Макмиллана. Теорема Крафта. Теорема Макмиллана	2	2	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Оптимальное кодирование. Метод Хаффмана. Метод Фано	1	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Метод Шеннона для бернуллиевских источников. Энтропия. Теорема Шеннона	1	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Критерий разделимости побуквенного кодирования. Теоремы Маркова. Алгоритм распознавания разделимости кода	2	2	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Код Левенштейна. Адаптивные методы сжатия данных. Код «стопка книг». Методы Лемпела — Зива и их модификации. Адаптивный метод Хаффмана. Арифметический код	2	2	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Раздел 3 «Криптология»				
Теорема Шеннона о существовании совершенно секретных шифров	1	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения,

				следуя общей форме проведения практических занятий
Криптографические системы с открытыми ключами. Односторонняя функция с лазейкой. «Шарады» Меркля	0,5	0,5	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма. Криптосистема Эль-Гамаля. Криптосистема Шамира	1,5	1,5	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Криптосистема RSA и проблема разложения числа на простые сомножители.	1	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Цифровая подпись	1	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Криптосистема Меркля — Хэллмана, основанная на задаче об укладке ранца	1	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Кодирующие системы Мак-Эллиса и Нидеррайтера	1	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Криптография на эллиптических кривых	1	1	1, 2, 3	Обучающиеся формируют знания и оттачивают умения, следуя общей форме проведения практических занятий
Итого:	**24**	**32**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на	Часы на	Часы на

		результаты обучения	выполнение	консультации
Семестр: 6				
1	Подготовка к практическим занятиям раздела 1 «Теория кодирования»	1, 2, 3	16	0
	Обучающиеся осуществляют обзор и разбор материалов лекций по соответствующей теме, запоминают основные определения и утверждения для подготовки к еженедельной пятиминутной письменной работы на проверку теоретических знаний текущего материала, выполняют еженедельное домашнее задание в виде письменного решения предложенных задач учебно-тренировочного плана.			
2	Подготовка к практическим занятиям раздела 2 «Сжатие данных»	1, 2, 3	8	0
	Обучающиеся осуществляют обзор и разбор материалов лекций по соответствующей теме, запоминают основные определения и утверждения для подготовки к еженедельной пятиминутной письменной работы на проверку теоретических знаний текущего материала, выполняют еженедельное домашнее задание в виде письменного решения предложенных задач учебно-тренировочного плана.			
3	Подготовка к практическим занятиям раздела 3 «Криптология»	1, 2, 3	8	0
	Обучающиеся осуществляют обзор и разбор материалов лекций по соответствующей теме, запоминают основные определения и утверждения для подготовки к еженедельной пятиминутной письменной работы на проверку теоретических знаний текущего материала, выполняют еженедельное домашнее задание в виде письменного решения предложенных задач учебно-тренировочного плана.			
4	Подготовка к контрольной работе	1, 2, 3	4	0
	Повторение материалов лекций по разделу «Теория кодирования», разбор решений типовых задач по материалам практических занятий.			
5	Подготовка к коллоквиуму по теории кодирования	1, 2, 3	8	0
	Обучающиеся осуществляют обзор и разбор материалов лекций соответствующего раздела, запоминают основные определения, формулировки утверждений, а также схемы доказательств ключевых утверждений. Выполняют подготовку к ответам по вопросам, представленным в фонде оценочных средств, являющихся приложением к рабочей программе дисциплины.			
6	Подготовка к коллоквиуму по сжатию данных	1, 2, 3	4	0
	Обучающиеся осуществляют обзор и разбор материалов лекций соответствующего раздела, запоминают основные определения, формулировки утверждений, а также схемы доказательств ключевых утверждений. Выполняют подготовку к ответам по вопросам, представленным в фонде оценочных средств, являющихся приложением к рабочей программе дисциплины.			
7	Подготовка к коллоквиуму по криптологии	1, 2, 3	4	0
	Обучающиеся осуществляют обзор и разбор материалов лекций соответствующего раздела, запоминают основные определения, формулировки утверждений, а также схемы доказательств ключевых утверждений. Выполняют подготовку к ответам по вопросам, представленным в фонде оценочных средств, являющихся приложением к рабочей программе дисциплины.			
8	Подготовка к экзамену	1, 2, 3	24	2

Подготовка к экзамену по вопросам, представленным в фонде оценочных средств, являющихся приложением к рабочей программе дисциплины.			
Итого		**76**	**2**

5. Образовательные технологии

В ходе реализации учебного процесса по дисциплине «Введение в теорию кодирования» проводятся лекционные и практические занятия, осуществляется индивидуальная и коллективная работа студентов, как в ходе семинарских занятий, так и при выполнении домашних упражнений. Темы, рассматриваемые на лекциях и изучаемые самостоятельно, закрепляются на семинарах, по вопросам, вызывающим затруднения, проводятся консультации.

Весь объем теоретического материала по дисциплине рассматривается в течение предусмотренного цикла лекций. Семинарские занятия призваны повысить понимание технической стороны изучаемых методов, алгоритмов и протоколов, а также рассмотреть механику применения теоретических результатов на практике.

Начало каждого семинара предусматривает выполнение письменной пятиминутной работы на знание определений, понятий и основных теоретических результатов, используемых на данном семинаре. Результаты и трудности, вызываемые письменной работой, обсуждаются сразу после ее окончания. Дискуссии на тему применимости нетривиальных теоретических результатов позволяют стимулировать интерес студента к предмету, изучить предмет глубже и всесторонне, а также помогают отслеживать темпы нарастания теоретических познаний по предмету от семинара к семинару. Далее следует разбор моментов в решении задач, вызвавших затруднения при выполнении домашнего задания. Далее работа на семинаре складывается из совместного с аудиторией выполнения базовых практических заданий, а впоследствии из индивидуальной работы студентов над заданиями средней и повышенной трудности.

В течение семестра по завершению каждого из основных разделов по теории кодирования, сжатию данных и криптологии предусмотрены коллоквиумы, в рамках которых студенты показывают свои теоретические знания в устной беседе с преподавателем.

В конце семестра проводится устное экзаменационное испытание, на котором студенту предлагается билет с двумя вопросами по материалам лекций и одно практическое задание среднего уровня сложности.

Для организации самостоятельной работы студентов, а также информирования о текущих достижениях в ходе изучения дисциплины применяются информационно-коммуникационные технологии (таблица 5.1).

Таблица 5.1

Информирование	Таблица текущих достижений студентов при изучении дисциплины «Введение в теорию кодирования». Таблица пересоздается каждый новый семестр и, соответственно, адрес ссылки меняется. https://docs.google.com
Консультирование	Личная почта преподавателей
Размещение учебных материалов	Веб-сайт: http:\\codingtheory.nsu.ru

6. Правила аттестации студентов по учебной дисциплине

Текущий контроль по дисциплине «Введение в теорию кодирования» осуществляется в форме сдачи коллоквиумов по основным разделам дисциплины, в рамках которых студенты показывают свои теоретические знания в устной беседе с преподавателем. Результаты сдачи коллоквиумов оцениваются по шкале «неудовлетворительно»,

«удовлетворительно», «хорошо», «отлично» и составляют одно из условий успешного прохождения промежуточной аттестации.

Промежуточная аттестация по дисциплине «Введение в теорию кодирования» проводится по завершению периода ее освоения (семестра) в форме устного экзамена.

Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

В таблице 6.1 представлено соответствие форм аттестации заявляемым требованиям к результатам освоения дисциплины.

Коды компетенций ФГОС	**Результаты обучения**	**Формы аттестации**	
		1 этап - Коллоквиум	**2 этап - экзамен**
ОПК-8	**ОПК-8.1** Знать: алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения	+	+

Требования к структуре и содержанию портфолио, оценочные средства, а также критерии оценки сформированности компетенций и освоения дисциплины в целом, представлены в Фонде оценочных средств, являющемся приложением 1 к настоящей рабочей программе дисциплины.

7. Литература

1. Соловьева Ф. И. Введение в теорию кодирования: учеб. пособие. Новосибирск, 2011. 123 с. [Электронный ресурс]. - URL: http://tc.nsu.ru/uploads/codingtheory.pdf
2. Соловьева Ф. И., Лось А. В., Могильных И. Ю. Сборник задач по теории кодирования, криптологии и сжатию данных: учеб. пособие. Новосибирск, 2013. 100 с. [Электронный ресурс]. - URL: http://e-lib.nsu.ru/dsweb/Get/Resource-895/page001.pdf
3. Сидельников, В.М. Теория кодирования / В.М. Сидельников. - Москва: Физматлит, 2008. - 323 с. - ISBN 978-5-9221-0943-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=68384
4. Шеннон, К. Работы по теории информации и кибернетике / К. Шеннон; под ред. Р. Л. Добрушина, О. Б. Лупанова; предисл. А. Н. Колмогорова. - Москва: Издательство иностранной литературы, 1963. - 830 с.: ил.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=450093

Интернет-ресурсы

Таблица 7.1

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	Сайт «Теория кодирования в НГУ» [Электронный ресурс]. – Режим доступа: http://codingtheory.nsu.ru	В помощь студентам разработан и постоянно совершенствуется сайт «Теория кодирования в НГУ» (http://www.codingtheory.nsu.ru), сайт содержит информацию и список литературы по всем разделам данной дисциплины.
2	Страница Потапова Владимира Николаевича [Электронный ресурс]. – Режим доступа: http://math.nsc.ru/~potapov	На сайте представлены учебные пособия по теории информации и сжатию данных.

8. Учебно-методическое и программное обеспечение дисциплины

8.1. Учебно-методическое обеспечение

- Соловьева Ф. И. Введение в теорию кодирования: Учеб. пособие 2-е изд. / Новосиб. гос. ун-т. Новосибирск, 2011. 124 с. Режим доступа: [http://tc.nsu.ru/uploads/codingtheory.pdf]
- Соловьева Ф. И, Лось А. В., Могильных И. Ю. Сборник задач по теории кодирования, криптологии и сжатию данных: учебное пособие [для студентов Мех-мат. фак. и Фак. информ. технологий НГУ] / М-во образования и науки РФ, Новосиб. нац. исслед. гос. ун-т, Фак. информ. технологий — Новосибирск: Редакционно-издательский центр НГУ, 2013. 99 с. Режим доступа: [http://e-lib.nsu.ru/dsweb/Get/Resource-895/page001.pdf].

8.2. Программное обеспечение

Для обеспечения реализации дисциплины используется стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office.

Специализированное ПО не требуется.

9. Профессиональные базы данных и информационные справочные системы

1. Полнотекстовые журналы Springer Journals за 1997-2015 г., электронные книги (2005-2016 гг.), реферативная БД по чистой и прикладной математике zbMATH.
2. Электронной библиотека диссертаций Российской государственной библиотеки (ЭБД РГБ).
3. Полнотекстовые электронные ресурсы Freedom Collection издательства Elsevier (Нидерланды) в части их тематических блоков по компьютерным наукам и математике.
4. Электронные ресурсы Web of Science Core Collection (Thomson Reuters Scientific LLC.), Journal Citation Reports + ESI.
5. Электронные БД JSTOR (США) в разделе Mathematics & Statistics.
6. БД Scopus (Elsevier).
7. Лицензионные материалы на сайте eLibrary.ru

10. Материально-техническое обеспечение

Таблица 10.1

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для проведения лекционных занятий
2	Компьютерный класс (с выходом в Internet)	Для организации самостоятельной работы обучающихся

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

Лист актуализации рабочей программы дисциплины
«Введение в теорию кодирования»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного
1.	Актуализирована на 2020-2021 уч.год	22.07.2020 №77	

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
М.М. Лаврентьев
«03» июля 2019 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине Введение в теорию кодирования

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Программная инженерия и компьютерные науки

Квалификация: бакалавр

Форма обучения: очная Год обучения:3, семестр: 6

Форма аттестации	Семестр
Экзамен	6

Новосибирск 2019

Фонд оценочных средств промежуточной аттестации по дисциплине является **Приложением 1** к рабочей программе дисциплины «Введение в теорию кодирования», реализуемой в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 Информатика и вычислительная техника, направленность (профиль): Программная инженерия и компьютерные науки.

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением ученого совета факультета информационных технологий, протокол № 75 от 02.07.2019.

Разработчики:
Доцент кафедры дискретного анализа и исследований операций ФИТ,
кандидат физико-математических наук И. Ю. Могильных

Заведующий кафедрой дискретного анализа и исследований операций ФИТ,
доктор физико-математических наук В. Л. Береснев

Ответственный за образовательную программу:
доцент кафедры систем информатики ФИТ,
кандидат технических наук А. А. Романенко

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная аттестация по дисциплине «Теория кодирования» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Код	Компетенции, формируемые в рамках дисциплины «Введение в теорию кодирования»	Семестр 6	
		1 этап - коллоквиум	2 этап - экзамен
	ОПК-8 Способен разрабатывать алгоритмы и программы, пригодные для практического применения		
ОПК-8.1	Знать: алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения	+	+

Текущий контроль по дисциплине «Введение в теорию кодирования» осуществляется в форме сдачи коллоквиумов по основным разделам дисциплины, в рамках которых студенты показывают свои теоретические знания в устной беседе с преподавателем. Результаты сдачи коллоквиумов оцениваются по шкале «неудовлетворительно», «удовлетворительно», «хорошо», «отлично» и составляют одно из условий успешного прохождения промежуточной аттестации.

Промежуточная аттестация по дисциплине состоит из устного экзамена.

Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация по дисциплине состоит из устного экзамена по теоретическим вопросам и задачам из разных разделов курса:

—теория кодов, исправляющих ошибки в каналах связи с шумами;

—криптология;

—сжатие данных.

Необходимым условием для прохождения промежуточной аттестации является оценка «отлично», «хорошо», «удовлетворительно», полученная по результатам ответа на экзамене.

Экзамен проводится в устной форме. Во время проведения экзамена студенту разрешается использовать калькулятор. В процессе ответа на вопросы экзаменационного билета студенту могут быть заданы дополнительные вопросы по темам дисциплины.

2. Требования к структуре и содержанию фонда оценочных средств промежуточной аттестации по дисциплине

Перечень оценочных средств, применяемых на каждом этапе проведения промежуточной аттестации по дисциплине, представлен в таблице П1.3.

Таблица П1.2

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1-ый этап			
1	Коллоквиум	Средство контроля усвоения учебного материала раздела дисциплины, организованное как устное собеседование с преподавателем, на котором студенту предлагается ответить на два случайных вопроса по материалам лекций соответствующего раздела курса.	Вопросы по темам/разделам дисциплины
2	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект контрольных заданий по вариантам
2-ой этап - Экзамен			
1	Экзаменационный билет	Комплекс вопросов и задач	Список теоретических вопросов и задач

2.1.1 Требования к структуре и содержанию контрольной работы

Контрольная работа состоит из 5 задач практического плана легкого и среднего уровня сложности, а также от одной до трех задач теоретического плана повышенной сложности. Все задания контрольной работы укладываются в рамки предложенного студентам на лекциях теоретического материа-

ла и могут быть выполнены на основе знаний, полученных на семинарских занятиях.

Примерный вариант промежуточной контрольной работы по разделу «Теория кодов, исправляющих ошибки»:

ВАРИАНТ 1

1. Постройте таблицу синдромов для троичного кода с порождающей матрицей

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

   Исправьте ошибки в векторе $y = (10021)$. Найдите параметры кода. Укажите пример ошибок, приводящих к неправильному декодированию.
2. Двоичный код C длины 7 имеет порождающий многочлен $g(x) = (x+1)(x^3+x+1)$.
   а) Найдите параметры кода C. Выпишите порождающую матрицу через $g(x)$.
   б) Найдите первый систематический кодер и закодируйте блок (101).
   в) С помощью второго систематического кодера закодируйте блок (110).
3. Постройте $GF(2^3)$, используя $x^3 + x + 1$. Вычислите $(110)^{23}(101)^4(011)^{2012}$.
4. Разложите многочлен $x^7 - 1$ на неприводимые над $GF(2)$ множители. Выпишите в явном виде минимальные многочлены, используя поле из задачи 3.
5. Найдите порождающий многочлен двоичного кода БЧХ длины 7 с конструктивным расстоянием $\delta = 3$. Определите его параметры.
6. Разложите многочлен $x^{11} - 1$ на неприводимые над $GF(3)$ множители.
7. Докажите, что $\deg \mu(x) \leqslant m$, где $\mu(x)$ – мин. многочлен элемента $\beta \in GF(p^m)$.

Полный список практических задач, доступных как для работы на семинарах, так и для контрольной работы, приведен в учебном пособии, составленном и изданном специально в помощь студентам при изучении данного курса: Ф. И. Соловьева, А. В. Лось, И. Ю. Могильных «Сборник задач по теории кодирования, криптологии и сжатию данных», Новосибирский гос. ун-т., Новосибирск, 2013, 100 с.

2.1.2 Требования к структуре и содержанию коллоквиума

Каждый из коллоквиумов представляет собой промежуточный контроль знаний по отдельному разделу курса: теории кодирования, криптологии или сжатию данных. На коллоквиуме студенту предлагается подготовить за один час ответ на два случайных теоретических вопроса из соответствующего раздела курса, а также решить задачу среднего уровня сложности. Вопросы для коллоквиума совпадают с вопросами из соответствующего раздела курса, предлагаемые к экзамену. На ответ отводится 15 – 20 дополнительных минут, в которые студент подробно излагает свои знания в непосредственной беседе с преподавателем, а также демонстрирует полноту и точность решения задачи.

ВОПРОСЫ К КОЛЛОКВИУМУ КУРСА "ВВЕДЕНИЕ В ТЕОРИЮ КОДИРОВАНИЯ"

1. Код, длина, мощность, кодовое расстояние. Число ошибок, которые исправляет код. Теорема Шеннона (без доказательства).
2. Код, его параметры. Двоичный симметричный канал связи с шумами, принцип максимума правдоподобия.
3. Линейный код, порождающая матрица, проверочная матрица, кодовое расстояние линейного кода. Канонический вид проверочной и порождающий матриц
теорема о матрицах, заданных в каноническом виде. Теорема о столбцах проверочной матрицы.
4. Теорема о столбцах проверочной матрицы, двоичный и q-значный код Хэмминга
5. Граница Хэмминга. Совершенный код, теорема Зиновьева-Леонтьева-Титвайнена. Граница Синглтона, примеры кодов достигающих границы Синглтона.
6. Граница Плоткина
7. Граница Варшамова-Гилберта
8. Конструкция Плоткина, расширение и выкалывание кодов.
10. Способы построения кодов из существующих: расширением кода добавлением проверки на четность, выкалыванием, укорочением, пополнением и выбрасыванием.
11. Конструкция Васильева совершенных кодов. Нелинейные совершенные коды.
12. Декодирование линейных кодов. Кодер, кодеры для линейных кодов через порождающую матрицу.
Декодирование линейных кодов: таблица стандартного расположения
13. Кодер, кодеры для линейных кодов через порождающую матрицу. Смежный класс по линейному коду, лидер смежного класса. Синдром, его свойства. Декодирование линейных кодов: таблица синдромов.
14. Вероятность ошибки декодирования для линейных кодов. Декодирование линейных кодов: таблица синдромов.
15. Конечное поле, характеристика поля. Теорема: порядок поля через его характеристику. Идеал кольца. Поле Галуа как фактор-кольцо (без доказательства).
16. Теорема о цикличности мультипликативной группы поля Галуа, следствия: теорема Ферма и число примитивных элементов поля Галуа.
17. Циклический код, циклический код как идеал фактор-кольца по x^n-1. Порождающий многочлен циклического кода, его единственность.
Теорема: выражение для кодовых слов кода через порождающий многочлен.
18. Порождающий многочлен циклического кода. Необходимое и достаточное условие существования циклического кода с порождающим g(x)
19. Необходимое и достаточное условие существования циклического кода с порождающим g(x), порождающая матрица циклического кода.

20. Систематические кодеры, первый и второй систематический кодер для циклического кода, несистематический кодер
21. Минимальный многочлен элемента поля Галуа, его свойства
22. Теорема о нулях кода, граница БЧХ
23. Граница БЧХ
24. Граница БЧХ, коды БЧХ
25. Граница БЧХ (без доказательства). Коды БЧХ, двоичные коды БЧХ, их параметры
26. Двоичный коды БЧХ, код Хэмминга как код БЧХ
27. Коды Рида-Соломона, их параметры и применение.

2.1.3 Требования к структуре и содержанию экзаменационного билета
В состав экзаменационного билета входят два теоретических вопроса и задача среднего уровня сложности из разных разделов курса:

— Теории кодирования;
— Сжатия данных;
— Криптологии.

Форма и перечень вопросов экзаменационного билета

Форма экзаменационного билета

Таблица П1.3

Новосибирский государственный университет
Экзамен

Введение в теорию кодирования
наименование дисциплины

09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Программная инженерия и компьютерные науки
наименование образовательной программы

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №

1. Случайный вопрос из одного из разделов курса.
2. Случайный вопрос из одного из разделов курса, несовпадающего с разделом, определенным первым вопросом данного билета.
3. Случайная задача из одного из разделов курса, несовпадающего с разделами, определенными вопросами данного билета.

Составитель: _____И. Ю. Могильных
(подпись)

Ответственный за образовательную программу:

_____ А. А. Романенко
(подпись)

«____»_____20 г.

Перечень вопросов экзамена, структурированный по разделам курса, представлен в таблице П1.4

Таблица П1.4

Раздел курса	Формулировка вопроса
Теория кодирования (ОПК-8)	Модель канала связи, скорость кода, пропускная способность
	Теорема Шеннона
	Вероятность ошибки декодирования. Стандартное расположение. Синдром.
	Поле Галуа, его свойства.
	Линейные коды. Кодирование и декодирование.
	Общие свойства линейных кодов. Теорема о связи проверочной и порождающей матриц.
	Теорема Глаголева.
	Границы объема кода: граница Синглтона, граница Хэмминга, граница Варшамова — Гилберта.
	Методы построения новых кодов из заданных. Комбинирование кодов.
	Теорема Плоткина. Каскадная конструкция.
	Совершенные коды. Теорема о существовании совершенных кодов.
	Коды Хэмминга над GF(q), способы задания, кодирование, декодирование, единственность.
	Конструкция кодов Васильева. Оценки числа совершенных кодов.
	Циклические коды. Кольцо многочленов над полем Галуа. Определение циклического кода.
	Теорема о необходимом и достаточном условии существования циклического кода с порождающим многочленом g(x).
	Кодирование циклических кодов.
	Декодирование циклических кодов.
	Существование циклического представления кода Хэмминга.
	Двоичные коды Боуза — Чоудхури — Хоквингема (БЧХ-коды).
	q-значные коды Боуза — Чоудхури — Хоквингема.
	Коды Рида-Соломона.
Сжатие данных (ОПК-8)	Разделимые и префиксные коды. Стоимость кодирования.
	Неравенство Крафта — Макмиллана. Теорема Крафта.
	Неравенство Крафта — Макмиллана. Теорема Макмиллана.

	Оптимальное кодирование. Метод Хаффмена.
	Метод Фано.
	Энтропия. Метод Шеннона для бернуллиевских источников.
	Теорема Шеннона.
	Критерий разделимости побуквенного кодирования. Теоремы Маркова. Алгоритм распознавания разделимости.
	Универсальное кодирование, теорема Фитингофа.
	Код Левенштейна.
	Код «стопка книг».
	Адаптивные методы сжатия данных.
	Методы Лемпела — Зива и их модификации.
	Адаптивный метод Хаффмена.
	Арифметический код.
Криптология (ОПК-8)	Введение в криптологию. Секретность и имитостойкость. Основные идеи.
	Криптография и криптоанализ.
	Криптографические системы с секретными ключами. Подстановки. Перестановки.
	Полиалфавитные шифры. Шифр с бегущим ключом. Криптографические системы коды.
	Теорема Шеннона о существовании совершенно секретных шифров.
	Криптосистема AES (стандарт шифрования данных).
	Российский стандарт шифрования данных ГОСТ.
	Криптосистема DES, схема Фейстеля.
	Криптографические системы с открытыми ключами. Односторонняя функция с лазейкой.
	«Шарады» Меркля.
	Криптосистема Диффи — Хэллмана и проблема вычисления дискретного логарифма.
	Криптосистема Шамира.
	Криптосистема RSA и проблема разложения числа на простые сомножители.
	Криптосистема Меркля — Хэллмана, основанная на задаче об укладке ранца.
	Кодирующие системы Мак-Эллиса и Нидеррайтера.
	Цифровая подпись.
	Введение в криптологию. Секретность и имитостойкость. Основные идеи.
	Криптография и криптоанализ.

Набор экзаменационных билетов формируется и утверждается в установленном порядке в начале учебного года при наличии контингента обучающихся, завершающих освоение дисциплины «Введение в теорию кодирования» в текущем учебном году.

3. Критерии оценки сформированности компетенций в рамках промежуточной аттестации по дисциплине

Таблица П1.5

Шифр компетенций	Структурные элементы оценочных средств	Показатель сформированности	Не сформирован (2 балла)	Пороговый уровень (3 балла)	Базовый уровень (4 балла)	Продвинутый (5 баллов)
ОПК-8	Коллоквиум и экзамен	ОПК-8.1 Знать: алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения	Имеет фрагментарное представление об основных требованиях информационной безопасности при решении стандартных задач профессиональной деятельности	Имеет представление об основных требованиях информационной безопасности при решении стандартных задач профессиональной деятельности	Знает с некритичными ограничениями основные требования информационной безопасности при решении стандартных задач профессиональной деятельности	Демонстрирует знания в деталях основные требования информационной безопасности при решении стандартных задач профессиональной деятельности

4. Критерии выставления оценок по результатам промежуточной аттестации по дисциплине

Результаты промежуточной аттестации в 6 семестре определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Оценка «неудовлетворительно» выставляется, если хотя бы одна компетенция не сформирована.

Итоговая оценка G результатов промежуточной аттестации выставляется по следующей формуле:

$$G = \min\{G_{ct}, G_{dc}, G_c\},$$

где G_{ct} — оценка за ответ на экзамене на вопрос из раздела курса по теории кодирования, G_{dc} — оценка за ответ на экзамене на вопрос из раздела курса по сжатию данных, G_c — оценка за ответ на экзамене на вопрос из раздела курса по криптологии.

Лист актуализации фонда оценочных средств
промежуточной аттестации по дисциплине
«Введение в теорию кодирования»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного
1.	Актуализирован на 2020-2021 уч.год	22.07.2020 №77