Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра теоретической и прикладной информатики

“УТВЕРЖДАЮ”
ДЕКАН ФПМИ
д.т.н. Тимофеев В. С.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Основы теории информации и криптографии

Образовательная программа: 02.03.03 Математическое обеспечение и администрирование информационных систем, профиль: Математическое и программное обеспечение информационных технологий

Курс: 3, семестр : 5

Факультет прикладной математики и информатики,

		Семестр
№	**Вид деятельности**	**5**
1	Всего зачетных единиц (кредитов)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	47
4	Лекции, час.	18
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	14
8	Аттестация, час.	2
9	Консультации, час.	9
10	Самостоятельная работа, час.	97
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 02.03.03 Математическое обеспечение и администрирование информационных систем

ФГОС введен в действие приказом №222 от 12.03.2015 г. , дата утверждения: 07.04.2015 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 02.03.03 Математическое обеспечение и администрирование информационных систем

Рабочая программа обсуждена на заседании кафедры

ТПИ, протокол заседания кафедры №4 от 20.06.2017

Утверждена на совете факультета прикладной математики и информатики, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.т.н. Гультяева Т. А.

Заведующий кафедрой:

доцент, д.т.н. Чубич В. М.

Ответственный за образовательную программу:

заведующий кафедрой Чубич В. М.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОПК.2 способность применять в профессиональной деятельности знания математических основ информатики; *в части следующих результатов обучения*:**
з11. Знать алгоритмы кодирования
з12. Знать основные математические модели элементарных криптосистем
у8. Уметь рассчитывать основные теоретические показатели моделей сообщений
***Компетенция ФГОС*: ОПК.7 способность использовать знания основных концептуальных положений функционального, логического, объектно-ориентированного и визуального направлений программирования, методов, способов и средств разработки программ в рамках этих направлений; *в части следующих результатов обучения*:**
у4. Уметь разрабатывать программные приложения для решения поставленных задач в области криптографии
***Компетенция НГТУ*: ПК.11.В/П способность формировать суждения о проблемах современной информатики; *в части следующих результатов обучения*:**
з2. Знать основные системы защиты информации в России и в ведущих зарубежных странах

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	Формы организации занятий
Основы теории информации и криптографии	
ОПК.2.у8 Уметь рассчитывать основные теоретические показатели моделей сообщений	
1.о вероятностно - статистических моделях сообщений и их свойства	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.2.з12 Знать основные математические модели элементарных криптосистем	
2.об основах экономного кодирования	Лекции; Лабораторные работы; Самостоятельная работа
3.об основах помехоустойчивого кодирования	Лекции; Лабораторные работы; Самостоятельная работа
4.о теоретических и практических основах криптографии	Лекции; Лабораторные работы; Самостоятельная работа
5.об основах теории чисел	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.2.у8 Уметь рассчитывать основные теоретические показатели моделей сообщений	
6.свойства вероятно-статистических моделях сообщений	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.2.з11 Знать алгоритмы кодирования	
7.алгоритмы побуквенного кодирования информации	Лекции; Лабораторные работы; Самостоятельная работа
8.алгоритмы помехоустойчивого кодирования информации	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.2.з12 Знать основные математические модели элементарных криптосистем	
9.основные математические модели элементарных криптосистем	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.2.з11 Знать алгоритмы кодирования	
10.алгоритмы генерации псевдослучайных последовательностей	Лекции; Лабораторные работы; Самостоятельная работа
11.методы тестирования чисел на простоту	Лекции; Лабораторные работы; Самостоятельная работа

12.методы решения сравнений	Лекции; Лабораторные работы; Самостоятельная работа
13.методы решения задачи дискретного логарифма	Лекции; Лабораторные работы; Самостоятельная работа
14.алгоритмы факторизации	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.2.у8 Уметь рассчитывать основные теоретические показатели моделей сообщений	
15.рассчитывать основные теоретические показатели моделей сообщений	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.7.у4 Уметь разрабатывать программные приложения для решения поставленных задач в области криптографии	
16.разрабатывать программные приложения для решения поставленных задач	Лабораторные работы; Самостоятельная работа
17.реализовывать алгоритмы, необходимые для решения поставленных задач	Лабораторные работы; Самостоятельная работа
ПК.11.В/П.з2 Знать основные системы защиты информации в России и в ведущих зарубежных странах	
18.основные системы защиты информации	Лекции; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 5				
Дидактическая единица: Основные аспекты теории информации (Вероятностно - статистические модели сообщений и их свойства)				
1. Тема 1. Основные аспекты теории информации. Введение в теорию информации. Задачи, решаемые в рамках теории информации. Вероятностно -статистические модели сообщений и их свойства. Вероятностно - статистические модели сообщений и их свойства. Собственная информация. Взаимная информация. Энтропия. Условная энтропия. Избыточность. Количество информации по К. Шеннону и его свойства.	0	4	1, 15, 6	Изучение задач, решаемые в рамках теории информации. Вероятностно-статистические модели сообщений и их свойства. Источники дискретных сообщений и их вероятностные модели. Собственная информации. Взаимная информация. Энтропия. Условная энтропия. Избыточность
Дидактическая единица: Основные принципы кодирования (Основы экономного кодирования. , Алгоритмы побуквенного кодирования информации, Основы помехоустойчивого кодирования.)				

2. Тема 2. Основы экономного кодирования. Введение в теорию кодирования. Основы экономного кодирования. Сжатие без потерь информации. Сжатие с потерями информации. Кодеры, основанные на системе сжатия без потерь информации. Основные методы побуквенного кодирования. Код Хаффмана. Код Шеннона. Код Шеннона-Фано. Код Гильбера-Мура.	0	2	2, 7	Изучение основ экономного кодирования. Сжатие без потерь информации.Сжатие с потерями информации.Кодеры, основанные на системе сжатия без потерь информации.Основные методы побуквенного кодирования. Код Хаффмана. Код Шеннона.Код Шеннона-Фано. Код Гильбера-Мура.
3. Тема 3. Помехоустойчивое кодирование. Коды с обнаружением ошибок. Коды с исправлением ошибок. Линейные блоковые коды. Коды Хэмминга. Циклические коды.	0	2	3, 8	Изучение основы помехоустойчивого кодирование. Коды с обнаружением ошибок.Коды с исправлением ошибок.Линейные блоковые коды.Коды Хэмминга.Циклические коды
Дидактическая единица: Основы криптографии (Основные математические модели элементарных криптосистем, Основы криптографии.)				
4. Тема 4. Основы криптографии. Терминология и основные понятия криптологии. Основные аспекты криптографии. Основные аспекты криптоанализа. Шеноновские модели криптографии. Теоретико-информационные оценки стойкости симметричных криптосистем.	0	2	18, 4, 9	Изучение терминологии и основных понятия криптологии. Основные аспекты криптографии. Основные аспекты криптоанализа. Шеноновские модели криптографии. Теоретико-информационные оценки стойкости симметричных криптосистем
Дидактическая единица: Математические основы криптологии (Основные положения теории чисел, Алгоритмы генерации псевдослучайных последовательностей, Методы тестирования чисел на простоту, Методы решения сравнений, Методы решения задачи дискретного логарифма, Алгоритмы факторизации.)				

5. Тема 5. Псевдолучайные последовательности. Равномерно распределенная случайная последовательность. Алгоритмы генерации псевдослучайных последовательностей. Конгруэнтные генераторы. Линейные и мультипликативные конгруэнтные генераторы. Нелинейные конгруэнтные генераторы. Квадратичные конгруэнтные генераторы. Генератор Эйхенауэра - Лена с обращением. Конгруэнтный генератор, использующий умножение с переносом. Рекуренты в конечном поле. Последовательности, порождаемые линейными регистрами сдвига с обратной связью. Генераторы Фибонначи. Криптостойкие генераторы на основе односторонних функций. Криптостойкие генераторы, основанные на проблемах теории чисел. Методы "улучшения" элементарных псевдослучайных последовательностей. Комбинирование алгоритмов генерации методом Макларена - Марсальи. Комбинирование LFSR-генераторов. Комбинирование с помощью псевдослучайного прореживания. Конгруэнтный генератор со случайными параметрами	0	2	10, 4	Изучение теории, связанной с псевдослучайными последовательностями. Равномерно распределенная случайная последовательность. Алгоритмы генерации псевдослучайных последовательностей.
6. Тема 6. Тестирование чисел на простоту и построение больших простых чисел. Метод пробных делений. Решето Эратосфена. Критерий Вильсона. Тест на ос-нове малой теоремы Ферма. Тест Соловея - Штрассена. Тест Леманна. Тест Рабина - Миллера. Полиномиальный тест распознавания простоты. Тест Конягина - Померанса. Метод Михалеску	0	2	11, 4, 5	Изучение алгоритмов тестирования чисел на простоту и построение больших простых чисел.

7. Тема 7. Теория сравнения Арифметика вычетов. Функция Эйлера. Сравнение первой степени. Решение сравнения первой степени с использованием алгоритма Евклида. Решение сравнения первой степени с использованием расширенного алгоритма Евклида. Решение сравнения способ Эйлера. Первообразные корни. Дискретные логарифмы в конечном поле.	0	2	12, 13, 4, 5	Изучение основ теория сравнения. Арифметика вычетов. Функция Эйлера. Изучение способов решения сравнение первой степени. Решение сравнения первой степени с использованием алгоритма Евклида. Решение сравнения первой степени с использованием расширенного алгоритма Евклида. Решение сравнения способ Эйлера. Изучение способов нахождения первообразных корней. Изучение способов решения задачи дискретного логарифма в конечном поле.
8. Тема 8. Разложение на множители (факторизация) Метод Ферма. Ро- факторизация Полларда. Метод Ро-Полларда. Метод Шермана-Лемана. Метод Ленстры.	0	1	11, 14, 4, 5	Изучение алгоритмов разложение на множители (факторизация).
9. Тема 8. Примеры систем шифрования, основанные на проблемах теории чисел Система шифрования RSA. Система шифрования Диффи-Хеллмана.	0	1	18, 4	Изучение примеров систем шифрования, основанные на проблемах теории чисел.Система шифрования RSA. Система шифрования Диффи-Хеллмана. Иметь представление о вычислениях в поле Галуа.

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 5				
Дидактическая единица: Основные аспекты теории информации (Вероятностно - статистические модели сообщений и их свойства)				
1. Решение типовых задач по теме "Основные аспекты теории информации"	2	4	1, 15, 16, 6	Приобретение навыка решения практических задач, отражающих основные свойства источников дискретных сообщений (ИДС).
Дидактическая единица: Основные принципы кодирования (Основы экономного кодирования. , Алгоритмы побуквенного кодирования информации, Основы помехоустойчивого кодирования.)				
2. Основные методы побуквенного кодирования	2	3	16, 17, 2, 7	Освоение основных алгоритмов побуквенного кодирования. Приобретение навыка реализации одного из алгоритмов побуквенного кодирования (согласно варианту).

3. Помехоустойчивое кодирование	2	2	16, 17, 3, 8	Освоение основных алгоритмов помехоустойчивого кодирования. Приобретение навыка реализации алгоритма обнаружения ошибок (контроль четности) и исправления ошибок (алгоритм Хэмминга).
Дидактическая единица: Основы криптографии (Основные математические модели элементарных криптосистем, Основы криптографии.)				
4. Шифры перестановки и замены	2	2	16, 17, 4, 9	Освоение основных алгоритмов шифрования перестановки и замены. Приобретение навыка реализации одного из алгоритмов шифрования перестановкой и заменой (согласно варианту).
Дидактическая единица: Математические основы криптологии (Основные положения теории чисел, Алгоритмы генерации псевдослучайных последовательностей, Методы тестирования чисел на простоту, Методы решения сравнений, Методы решения задачи дискретного логарифма, Алгоритмы факторизации.)				
5. Генерирование равномерно распределенных псевдослучайных последовательностей	2	2	10, 16, 17, 4	Освоение основных алгоритмов программной генерации равномерно распределенных псевдослучайных последовательностей. Приобретение навыка реализации одного из алгоритмов генерации равномерно распределенных псевдослучайных последовательностей. Приобретение навыка вычисления основных свойств полученной последовательности.
6. Тестирование чисел на простоту и построение больших простых чисел	2	2	11, 12, 16, 17, 5	Освоение основных программных методов тестирования чисел на простоту. Приобретение навыка реализации одного из алгоритмов тестирования чисел на простоту (согласно варианту).
7. Факторизация составного числа	2	3	12, 13, 14, 16, 17, 5	Освоение простых алгоритмов факторизации составного числа. Приобретение навыка реализации одного из алгоритмов факторизации составного числа (согласно варианту).

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 5				
1	РГЗ	14, 2, 3, 7, 8	17	2
Проектирование и разработка программного приложения: Гультяева Т. А. Расчетно-графическая работа по курсу "Основы теории информации и криптографии" [Электронный ресурс] : учебно-методическое пособие / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21805_1326688460.doc. - Загл. с экрана. Гультяева Т. А. Основы теории информации и криптографии [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234869. - Загл. с экрана.			
2	Подготовка к занятиям	1, 10, 11, 12, 13, 14, 15, 16, 17, 2, 3, 4, 5, 6, 7, 8, 9	70	4
Проработка лекционного материала, подготовка к тестам, подготовка к лабораторным работам: Основы теории информации и криптографии : методические указания к выполнению лабораторных работ для 3 курса образовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль Математическое и программное обеспечение информационных технологий факультета прикладной математики и иформатики / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2017. - 68, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235026 Основы теории информации и криптографии. Ч. 1 : методические указания к выполнению лабораторных работ для 3 курса ФПМИ по специальностям "Математическое обеспечение и администрирование информационных систем" (010503), "Прикладная информатика в менеджменте" (080801) / Новосиб. гос. техн. ун-т ; [сост. Т. А. Гультяева]. - Новосибирск, 2006. - 27, [1] с.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2007/3315.rar Основы теории информации и криптографии. Ч. 2 : [методические указания к выполнению лабораторных работ для 3 курса ФПМИ по специальностям 010503 - Математическое обеспечение и администрирование информационных систем, 080801 - Прикладная информатика в менеджменте] / Новосиб. гос. техн. ун-т ; [сост. Т. А. Гультяева]. - Новосибирск, 2009. - 41, [2] с. : ил., табл.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2009/3623.pdf Гультяева Т. А. Основы теории информации и криптографии [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234869. - Загл. с экрана. Основы теории информации и криптографии : методические указания к выполнению лабораторных работ для 3 курса ФПМИ по специальности "Математическое обеспечение и администрирование информационных систем" (010500.62) / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2015. - 68, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000216623			
3	Подготовка к аттестации	1, 10, 11, 12, 13, 14, 15, 18, 2, 3, 4, 5, 6, 7, 8, 9	10	3

Консультации с преподавателем: Основы теории информации и криптографии : методические указания к выполнению лабораторных работ для 3 курса образовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль Математическое и программное обеспечение информационных технологий факультета прикладной математики и иформатики / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2017. - 68, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235026 Основы теории информации и криптографии. Ч. 1 : методические указания к выполнению лабораторных работ для 3 курса ФПМИ по специальностям "Математическое обеспечение и администрирование информационных систем" (010503), "Прикладная информатика в менеджменте" (080801) / Новосиб. гос. техн. ун-т ; [сост. Т. А. Гультяева]. - Новосибирск, 2006. - 27, [1] с.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2007/3315.rar Основы теории информации и криптографии. Ч. 2 : [методические указания к выполнению лабораторных работ для 3 курса ФПМИ по специальностям 010503 - Математическое обеспечение и администрирование информационных систем, 080801 - Прикладная информатика в менеджменте] / Новосиб. гос. техн. ун-т ; [сост. Т. А. Гультяева]. - Новосибирск, 2009. - 41, [2] с. : ил., табл.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2009/3623.pdf Гультяева Т. А. Расчетно-графическая работа по курсу "Основы теории информации и криптографии" [Электронный ресурс] : учебно-методическое пособие / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21805_1326688460.doc. - Загл. с экрана. Гультяева Т. А. Основы теории информации и криптографии [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234869. - Загл. с экрана. Основы теории информации и криптографии : методические указания к выполнению лабораторных работ для 3 курса ФПМИ по специальности "Математическое обеспечение и администрирование информационных систем" (010500.62) / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2015. - 68, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000216623

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	Личный типовой сайт:http://ami.nstu.ru/~gultyaeva
Консультирование	e-mail:t.gultyaeva@corp.nstu.ru
Размещение учебных материалов	Личный типовой сайт:http://ami.nstu.ru/~gultyaeva

Таблица 5.2

Активные и интерактивные формы проведения занятий

№	Наименование активных форм	Коды формируемых компетенций
1	Метод проектов	ОПК.2; ОПК.7;
Формируемые умения: з11. Знать алгоритмы кодирования; з12. Знать основные математические модели элементарных криптосистем; у4. Уметь разрабатывать программные приложения для решения поставленных задач в области криптографии; у8. Уметь рассчитывать основные теоретические показатели моделей сообщений		
Краткое описание применения: Выполненнение лабораторной работы является проектом для студента.		

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 5		
Лабораторная:	20	40
Контролирующие материалы (список вопросов) приводятся в "Основы теории информации и криптографии : методические указания к выполнению лабораторных работ для 3 курса образовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль Математическое и программное обеспечение информационных технологий факультета прикладной математики и иформатики / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2017. - 68, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235026"		
РГЗ:	10	20
Контролирующие материалы (Защита в виде обсуждения) приводятся в "Гультяева Т. А. Расчетно-графическая работа по курсу "Основы теории информации и криптографии" [Электронный ресурс] : учебно-методическое пособие / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21805_1326688460.doc. - Загл. с экрана."		
Экзамен:	20	40
Контролирующие материалы (список вопросов) приводятся в "Гультяева Т. А. Основы теории информации и криптографии [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234869. - Загл. с экрана."		

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля	
		Защита РГЗ	Экзамен
ОПК.2	з11. Знать алгоритмы кодирования	+	+
	з12. Знать основные математические модели элементарных криптосистем		+
	у8. Уметь рассчитывать основные теоретические показатели моделей сообщений		+
ОПК.7	у4. Уметь разрабатывать программные приложения для решения поставленных задач в области криптографии	+	
	ПК.11.В/П з2. Знать основные системы защиты информации в России и в ведущих зарубежных странах		+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Гультяева Т. А. Основы теории информации и криптографии : конспект лекций / Т. А. Гультяева; Новосиб. гос. техн. ун-т. - Новосибирск, 2010. - 86, [1] с. : ил.. - Режим доступа: http://www.ciu.nstu.ru/fulltext/textbooks/2010/gultyaeva.pdf

2. Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности : [учебное пособие для вузов по специальностям 090102 (075200) - "Компьютерная безопасность" и др.] / С. В. Запечников. - М., 2007. - 319 с. : ил.

3. Глухов, М.М. Введение в теоретико-числовые методы криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — СПб. : Лань, 2011. — 400 с. — Режим доступа: http://e.lanbook.com/book/68466 — Загл. с экрана.

4. Основы теории информации и криптографии. Ч. 1 : методические указания к выполнению лабораторных работ для 3 курса ФПМИ по специальностям "Математическое обеспечение и администрирование информационных систем" (010503), "Прикладная информатика в менеджменте" (080801) / Новосиб. гос. техн. ун-т ; [сост. Т. А. Гультяева]. - Новосибирск, 2006. - 27, [1] с.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2007/3315.rar

5. Основы теории информации и криптографии. Ч. 2 : [методические указания к выполнению лабораторных работ для 3 курса ФПМИ по специальностям 010503 - Математическое обеспечение и администрирование информационных систем, 080801 - Прикладная информатика в менеджменте] / Новосиб. гос. техн. ун-т ; [сост. Т. А. Гультяева]. - Новосибирск, 2009. - 41, [2] с. : ил., табл.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2009/3623.pdf

Дополнительная литература

1. Математические и компьютерные основы криптологии : учеб. пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. – М. : Новое знание, 2003. – 384 с.

2. Фомичев В. М. Методы дискретной математики в криптологии / В. М. Фомичев. – М. : Диалог-МИФИ, 2010. – 424 с.

3. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – 2-е изд., доп. – М. : МЦНМО, 2006 – 336 с.

4. Шнайер Б. Прикладная криптография : Протоколы, алгоритмы, исход. тексты на яз. Си / Б. Шнайер. – М. : Триумф, 2002. – 815 с. : ил. – (Знания и опыт экспертов).

5. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии : учеб. пособие для студентов, обучающихся по специальности "Компьютер. безопасность" / А. В. Черемушкин. – [М.] : МЦНМО, 2002. – 103 с. : ил.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Гультяева Т. А. Основы теории информации и криптографии [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234869. - Загл. с экрана.

2. Основы теории информации и криптографии : методические указания к выполнению лабораторных работ для 3 курса образовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль Математическое и программное обеспечение информационных технологий факультета прикладной математики и иформатики / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2017. - 68, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235026

3. Гультяева Т. А. Расчетно-графическая работа по курсу "Основы теории информации и криптографии" [Электронный ресурс] : учебно-методическое пособие / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21805_1326688460.doc. - Загл. с экрана.

4. Основы теории информации и криптографии : методические указания к выполнению лабораторных работ для 3 курса ФПМИ по специальности "Математическое обеспечение и администрирование информационных систем" (010500.62) / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2015. - 68, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000216623

8.2 Специализированное программное обеспечение

1 Microsoft Office
2 Visual Studio
3 MathCAD
4 MathType
5 Maple 11

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Используется при демонстрации лекционного материала

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Используется для выполнения студентами лабораторных работ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра теоретической и прикладной информатики

“УТВЕРЖДАЮ”
ДЕКАН ФПМИ
д.т.н., доцент В.С. Тимофеев
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы теории информации и криптографии

Образовательная программа: 02.03.03 Математическое обеспечение и администрирование информационных систем, профиль: Математическое и программное обеспечение информационных технологий

Новосибирск 2015

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по дисциплине Основы теории информации и криптографии приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОПК.2 способность применять в профессиональной деятельности знания математических основ информатики	з11. Знать алгоритмы кодирования	Генерирование равномерно распределенных псевдослучайных последовательностей Основные методы побуквенного кодирования Помехоустойчивое кодирование Тема 2. Основы экономного кодирования. Введение в теорию кодирования. Основы экономного кодирования. Сжатие без потерь информации. Сжатие с потерями информации. Кодеры, основанные на системе сжатия без потерь информации. Основные методы побуквенного кодирования. Код Хаффмана. Код Шеннона. Код Шеннона-Фано. Код Гильбера-Мура. Тема 3. Помехоустойчивое кодирование. Коды с обнаружением ошибок. Коды с исправлением ошибок. Линейные блоковые коды. Коды Хэмминга. Циклические коды. Тема 5. Псевдолучайные последовательности. Равномерно распределенная случайная последовательность. Алгоритмы генерации псевдослучайных последовательностей. Конгруэнтные генераторы. Линейные и мультипликативные конгруэнтные генераторы. Нелинейные конгруэнтные генераторы. Квадратичные конгруэнтные генераторы. Генератор Эйхенауэра - Лена с обращением. Конгруэнтный генератор, использующий умножение с переносом. Рекуренты в конечном поле. Последовательности, порождаемые линейными регистрами сдвига с обратной связью. Генераторы Фибонначи. Криптостойкие	РГЗ	Экзамен: вопросы 11-26 Экзамен: задачи 18-54

		генераторы на основе односторонних функций. Криптостойкие генераторы, основанные на проблемах теории чисел. Методы "улучшения" элементарных псевдослучайных последовательностей. Комбинирование алгоритмов генерации методом Макларена - Марсальи. Комбинирование LFSR-генераторов. Комбинирование с помощью псевдослучайного прореживания. Конгруэнтный генератор со случайными параметрами Тема 6. Тестирование чисел на простоту и построение больших простых чисел. Метод пробных делений. Решето Эратосфена. Критерий Вильсона. Тест на ос-нове малой теоремы Ферма. Тест Соловея - Штрассена. Тест Леманна. Тест Рабина - Миллера. Полиномиальный тест распознавания простоты. Тест Конягина - Померанса. Метод Михалеску Тема 7. Теория сравнения Арифметика вычетов. Функция Эйлера. Сравнение первой степени. Решение сравнения первой степени с использованием алгоритма Евклида. Решение сравнения первой степени с использованием расширенного алгоритма Евклида. Решение сравнения способ Эйлера. Первообразные корни. Дискретные логарифмы в конечном поле. Тема 8. Разложение на множители (факторизация) Метод Ферма. Ро- факторизация Полларда. Метод Ро-Полларда. Метод Шермана-Лемана. Метод Ленстры. Тестирование чисел на простоту и построение больших простых чисел Факторизация составного числа		
ОПК.2	з12. Знать основные математические модели элементарных криптосистем	Генерирование равномерно распределенных псевдослучайных последовательностей Основные методы побуквенного кодирования Помехоустойчивое кодирование Тема 2. Основы экономного кодирования. Введение в теорию кодирования. Основы экономного кодирования. Сжатие без потерь		Экзамен: вопросы 27-82 Экзамен: задачи 55-117

		информации. Сжатие с потерями информации. Кодеры, основанные на системе сжатия без потерь информации. Основные методы побуквенного кодирования. Код Хаффмана. Код Шеннона. Код Шеннона-Фано. Код Гильбера-Мура. Тема 3. Помехоустойчивое кодирование. Коды с обнаружением ошибок. Коды с исправлением ошибок. Линейные блоковые коды. Коды Хэмминга. Циклические коды. Тема 4. Основы криптографии. Терминология и основные понятия криптологии. Основные аспекты криптографии. Основные аспекты криптоанализа. Шеноновские модели криптографии. Теоретико-информационные оценки стойкости симметричных криптосистем. Тема 5. Псевдолучайные последовательности. Равномерно распределенная случайная последовательность. Алгоритмы генерации псевдослучайных последовательностей. Конгруэнтные генераторы. Линейные и мультипликативные конгруэнтные генераторы. Нелинейные конгруэнтные генераторы. Квадратичные конгруэнтные генераторы. Генератор Эйхенауэра - Лена с обращением. Конгруэнтный генератор, использующий умножение с переносом. Рекуренты в конечном поле. Последовательности, порождаемые линейными регистрами сдвига с обратной связью. Генераторы Фибонначи. Криптостойкие генераторы на основе односторонних функций. Криптостойкие генераторы, основанные на проблемах теории чисел. Методы "улучшения" элементарных псевдослучайных последовательностей. Комбинирование алгоритмов генерации методом Макларена - Марсальи. Комбинирование LFSR-генераторов. Комбинирование с помощью псевдослучайного прореживания. Конгруэнтный генератор со случайными параметрами Тема 6.		

		Тестирование чисел на простоту и построение больших простых чисел. Метод пробных делений. Решето Эратосфена. Критерий Вильсона. Тест на ос-нове малой теоремы Ферма. Тест Соловея - Штрассена. Тест Леманна. Тест Рабина - Миллера. Полиномиальный тест распознавания простоты. Тест Конягина - Померанса. Метод Михалеску Тема 7. Теория сравнения Арифметика вычетов. Функция Эйлера. Сравнение первой степени. Решение сравнения первой степени с использованием алгоритма Евклида. Решение сравнения первой степени с использованием расширенного алгоритма Евклида. Решение сравнения способ Эйлера. Первообразные корни. Дискретные логарифмы в конечном поле. Тема 8. Примеры систем шифрования, основанные на проблемах теории чисел Система шифрования RSA. Система шифрования Диффи-Хеллмана. Тема 8. Разложение на множители (факторизация) Метод Ферма. Ро- факторизация Полларда. Метод Ро-Полларда. Метод Шермана-Лемана. Метод Ленстры. Тестирование чисел на простоту и построение больших простых чисел Факторизация составного числа Шифры перестановки и замены		
ОПК.2	у8. Уметь рассчитывать основные теоретические показатели моделей сообщений	Решение типовых задач по теме "Основные аспекты теории информации" Тема 1. Основные аспекты теории информации. Введение в теорию информации. Задачи, решаемые в рамках теории информации. Вероятностно - статистические модели сообщений и их свойства. Вероятностно - статистические модели сообщений и их свойства. Собственная информация. Взаимная информация. Энтропия. Условная энтропия. Избыточность. Количество информации по К. Шеннону и его свойства.		Экзамен: вопросы 1-10 Экзамен: задачи 1-17

ОПК.7 способность использовать знания основных концептуальных положений функционального, логического, объектно-ориентированного и визуального направлений программирования, методов, способов и средств разработки программ в рамках этих направлений	у4. Уметь разрабатывать программные приложения для решения поставленных задач в области криптографии	Генерирование равномерно распределенных псевдослучайных последовательностей Основные методы побуквенного кодирования Помехоустойчивое кодирование Тестирование чисел на простоту и построение больших простых чисел Факторизация составного числа Шифры перестановки и замены	РГЗ	
ПК.11.В/П способность формировать суждения о проблемах современной информатики	з2. Знать основные системы защиты информации в России и в ведущих зарубежных странах	Тема 4. Основы криптографии. Терминология и основные понятия криптологии. Основные аспекты криптографии. Основные аспекты криптоанализа. Шеноновские модели криптографии. Теоретико-информационные оценки стойкости симметричных криптосистем. Тема 8. Примеры систем шифрования, основанные на проблемах теории чисел Система шифрования RSA. Система шифрования Диффи-Хеллмана.		Экзамен: вопросы 27-30 Экзамен: вопросы 73-75

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 5 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОПК.2, ОПК.7.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 5 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОПК.2, ОПК.7, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра теоретической и прикладной информатики

Паспорт экзамена

по дисциплине «Основы теории информации и криптографии», 5 семестр

1. Методика оценки

Экзамен проводится в письменной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-31, второй вопрос из диапазона вопросов 32-82 (п. 4), третий: 1-39 (задачи п. 4), четвертый: 40-78 (задачи п. 4). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФПМИ

Билет № __1___
к экзамену по дисциплине «Основы теории информации и криптографии»

---

1. Код Шеннона

2. Решение сравнения первой степени с использованием расширенного алгоритма Евклида

3. Источник вырабатывает ансамбль сообщений *X*. Символы в последовательности независимы. Вычислить энтропию источника и определить избыточность.

$$X = \begin{Bmatrix} x_1 & x_2 & x_3 & x_4 \\ 0.2 & 0.3 & 0.4 & 0.1 \end{Bmatrix}$$

4. Построить LFSR-генератор, заданный многочленом $g(x) = x^7 + x^6 + x^4 + x^3$ и начальным состоянием 11001002, и получить последовательность, содержащую 10 бит.

Утверждаю: зав. кафедрой ____ _____ д.т.н.,проф. Чубич В.М.
(подпись)
(дата)

2. Критерии оценки

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки,

оценка составляет *от 0 до* 19 *баллов.*

- Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные, оценка составляет *от 20 до 30 баллов.*
- Ответ на экзаменационный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *от 31 до 34 баллов.*
- Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет *от 35 до 40 баллов.*

3. Шкала оценки

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** экзамену **по дисциплине** «Основы теории информации и криптографии»

Полный перечень вопросов к экзамену

1. Введение в теорию информации
2. Задачи, решаемые в рамках теории информации
3. Вероятностно - статистические модели сообщений и их свойства
4. Источники дискретных сообщений и их вероятностные модели
5. Собственная информация
6. Взаимная информация
7. Энтропия
8. Условная энтропия
9. Избыточность
10. Количество информации по Шеннону и его свойства
11. Введение в теорию кодирования
12. Основы экономного кодирования
13. Сжатие без потерь информации
14. Сжатие с потерями информации
15. Кодеры, основанные на системе сжатия без потерь информации
16. Основные методы побуквенного кодирования
17. Код Хаффмана
18. Код Шеннона
19. Код Шеннона-Фано
20. Код Гильбера-Мура
21. Помехоустойчивое кодирование
22. Коды с обнаружением ошибок
23. Коды с исправлением ошибок
24. Линейные блоковые коды
25. Коды Хэмминга

26. Циклические коды
27. Терминология и основные понятия криптологии
28. Основные аспекты криптографии
29. Основные аспекты криптоанализа
30. Шеноновские модели криптографии
31. Теоретико-информационные оценки стойкости симметричных криптосистем
32. Псевдослучайные последовательности
33. Равномерно распределенная случайная последовательность
34. Алгоритмы генерации псевдослучайных последовательностей
35. Конгруэнтные генераторы
36. Линейные и мультипликативные конгруэнтные генераторы
37. Нелинейные конгруэнтные генераторы
38. Квадратичные конгруэнтные генераторы
39. Генератор Эйхенауэра - Лена с обращением
40. Конгруэнтный генератор, использующий умножение с переносом
41. Рекуренты в конечном поле
42. Последовательности, порождаемые линейными регистрами сдвига с обратной связью
43. Генераторы Фибонначи
44. Криптостойкие генераторы на основе односторонних функций
45. Криптостойкие генераторы, основанные на проблемах теории чисел
46. Методы "улучшения" элементарных псевдослучайных последовательностей
47. Комбинирование алгоритмов генерации методом Макларена - Марсальи
48. Комбинирование LFSR-генераторов
49. Комбинирование с помощью псевдослучайного прореживания
50. Конгруэнтный генератор со случайными параметрами
51. Теория чисел
52. Простые числа
53. Тестирование чисел на простоту и построение больших простых чисел
54. Метод пробных делений
55. Решето Эратосфена
56. Критерий Вильсона
57. Тест на основе малой теоремы Ферма
58. Тест Соловея - Штрассена
59. Тест Леманна
60. Тест Рабина - Миллера
61. Полиномиальный тест распознавания простоты
62. Тест Конягина - Померанса
63. Метод Михалеску
64. Теория сравнения
65. Арифметика вычетов
66. Функция Эйлера
67. Сравнение первой степени
68. Решение сравнения первой степени с использованием алгоритма Евклида
69. Решение сравнения первой степени с использованием расширенного алгоритма Евклида
70. Решение сравнения способ Эйлера
71. Первообразные корни
72. Дискретные логарифмы в конечном поле
73. Примеры систем шифрования, основанные на проблемах теории чисел
74. Система шифрования RSA
75. Система шифрования Диффи-Хеллмана

76. Разложение на множители (факторизация)
77. Метод Ферма
78. $p-1$ - факторизация Полларда
79. Метод ρ-Полларда
80. Метод Шермана-Лемана
81. Метод Ленстры
82. Вычисление в поле Галуа

Полный перечень задач к экзамену

1. Дан ансамбль $\begin{pmatrix} a & b & c & d & e \\ 0.5 & 0.25 & 0.125 & 0.0625 & 0.0625 \end{pmatrix}$. Вычислить количество собственной информации I (a) = ?, I (b) = ? , I (c) = ? , I (d) = ? , I (e) = ?

2. Дан ансамбль $\begin{pmatrix} a & b & c & d & e \\ 0.2 & 0.25 & 0.35 & 0.15 & 0.05 \end{pmatrix}$. Вычислить количество собственной информации I (a) = ?, I (b) = ? , I (c) = ? , I (d) = ? , I (e) = ?

3. Дан ансамбль $\begin{pmatrix} a & b & c & d \\ 0.5 & 0.125 & 0.25 & 0.125 \end{pmatrix}$. Вычислить количество собственной информации I (a) = ?, I (b) = ? , I (c) = ? , I (d) = ?

4. Дан ансамбль $\begin{pmatrix} a & b & c & d \\ 0.1 & 0.25 & 0.35 & 0.3 \end{pmatrix}$. Вычислить количество собственной информации I (a) = ?, I (b) = ? , I (c) = ? , I (d) = ?

5. Дан ансамбль $\begin{pmatrix} a & b & c & d & e \\ 0.5 & 0.25 & 0.125 & 0.0625 & 0.0625 \end{pmatrix}$. Вычислить энтропию.

6. Дан ансамбль $\begin{pmatrix} a & b & c & d & e \\ 0.2 & 0.25 & 0.35 & 0.15 & 0.05 \end{pmatrix}$. Вычислить энтропию.

7. Дан ансамбль $\begin{pmatrix} a & b & c & d \\ 0.5 & 0.125 & 0.25 & 0.125 \end{pmatrix}$. Вычислить энтропию.

8. Дан ансамбль $\begin{pmatrix} a & b & c & d \\ 0.1 & 0.25 & 0.35 & 0.3 \end{pmatrix}$. Вычислить энтропию.

9. Источник вырабатывает ансамбль сообщений X. Символы в последовательности независимы. Вычислить энтропию источника и определить избыточность.
$X = \begin{Bmatrix} x_1 & x_2 & x_3 & x_4 \\ 0.2 & 0.3 & 0.4 & 0.1 \end{Bmatrix}$

10. Источник вырабатывает ансамбль сообщений B = <X, P>. Символы в последовательности независимы. Вычислить энтропию источника и определить избыточность.
X = (a, b, c, d, e), P = (0.4, 0.2, 0.2, 0.1, 0.1).

11. Источник вырабатывает ансамбль сообщений B = <X, P>. Символы в последовательности независимы. Вычислить энтропию источника и определить избыточность.
X = (a, b, c), P = (0.4, 0.5, 0.1).

12. Алфавит некоторого языка состоит из 32 букв, включая промежуток между буквами. Вычислить энтропию однобуквенного текста, считая вероятности появления любой из букв в заданном тексте одинаковыми.

13. На шахматной доске произвольным образом расставлены фигуры. Априори все положения фигур на доске одинаково вероятны. Определить собственную информацию, получаемую от сообщения, что фигура находится в одной из угловых клеток доски.

14. Символы азбуки Морзе могут появиться в сообщении с вероятностями: для точки – 0.51, для тире – 0.31, для промежутка между буквами – 0.12, между словами – 0.06. Определить среднее количество информации в сообщении из 500 символов данного алфавита, считая, что связь между последовательными символами отсутствует.

15. Измеряемое напряжение лежит в пределах от 0 до 6 В. Телеметрический датчик регистрирует приращение напряжения, равное 0.01 В. Найти наибольшее среднее количество информации, получаемое за 10 независимых измерений.

16. Из шести букв разрезной азбуки составлено слово "машина". Ребенок, не умеющий читать, рассыпал эти буквы и затем собрал в произвольном порядке. Какое количество информации будет содержаться в утверждении, что у него снова получилось слово "машина"?

17. Система радиозонда измеряет давление. Барометр имеет 10 отметок шкалы, и его отсчеты могут изменяться до любого допустимого значения за 0.01 с. Связь между отсчетами отсутствует. Найти энтропию источника за 1 с., если показания барометра будут появляться со следующими вероятностями:

Отметка шкалы	0	1	2	3	4	5	6	7	8	9
Вероятность	0.05	0.05	0.05	0.05	0.1	0.2	0.3	0.1	0.05	0.05

18. Перевести число 5.2310 в двоичную систему счисления с точностью до 1 / 28.

19. Перевести число 1.02510 в двоичную систему счисления с точностью до 1 / 28.

20. Перевести число 13.5110 в двоичную систему счисления с точностью до 1 / 28.

21. Перевести число 63.2510 в двоичную систему счисления с точностью до 1 / 28.

22. Перевести число 24.07510 в двоичную систему счисления с точностью до 1 / 28.

23. Перевести число 9.0110 в двоичную систему счисления с точностью до 1 / 28.

24. Перевести число 16.3510 в двоичную систему счисления с точностью до 1 / 28.

25. Перевести число 7.3310 в двоичную систему счисления с точностью до 1 / 28.

26. Построить код для ансамбля $A = \begin{Bmatrix} a & b & c & d & e \\ 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \end{Bmatrix}$, используя алгоритм Хаффмана.

27. Построить код для ансамбля $A = \begin{Bmatrix} a & b & c & d & e \\ 0.1 & 0.2 & 0.3 & 0.2 & 0.2 \end{Bmatrix}$, используя алгоритм Хаффмана.

28. Построить код для ансамбля $A = \begin{Bmatrix} a & b & c & d & e \\ 0.4 & 0.1 & 0.25 & 0.05 & 0.2 \end{Bmatrix}$, используя алгоритм Шеннона.

29. Построить код для ансамбля $A = \begin{Bmatrix} a & b & c & d & e \\ 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \end{Bmatrix}$, используя алгоритм Шеннона.

30. Построить код для ансамбля $A = \begin{Bmatrix} a & b & c & d & e \\ 0.1 & 0.2 & 0.4 & 0.1 & 0.2 \end{Bmatrix}$, используя алгоритм Шеннона-Фано.

31. Построить код для ансамбля $A = \begin{Bmatrix} a & b & c & d & e \\ 0.15 & 0.5 & 0.2 & 0.1 & 0.05 \end{Bmatrix}$, используя алгоритм Шеннона-Фано.

32. Построить код для ансамбля $A = \begin{Bmatrix} a & b & c & d & e \\ 0.4 & 0.3 & 0.15 & 0.12 & 0.03 \end{Bmatrix}$, используя алгоритм Гильбера-Мура.

33. Построить код для ансамбля $A=\begin{Bmatrix} a & b & c & d & e \\ 0.15 & 0.5 & 0.2 & 0.1 & 0.05 \end{Bmatrix}$, используя алгоритм Гильбера-Мура.

34. Найти кодовое расстояние кода (d0) для кодовых слов: 0010, 0001 и 1111.

35. Найти расстояние Хэмминга для кодовых слов: 0011 и 0100.

36. Найти расстояние Хэмминга для кодовых слов: 00100111 и 10110110.

37. Найти порождающую и проверочную матрицы для циклического кода, заданного следующим порождающим многочленом: $g(x)=x^2+x+1$ (n и k – выбрать самостоятельно).

38. Найти порождающую и проверочную матрицы для циклического кода, заданного следующим порождающим многочленом: $g(x)=x^4+x^2+1$ (n и k – выбрать самостоятельно).

39. Найти порождающую и проверочную матрицы для циклического кода, заданного следующим порождающим многочленом: $g(x)=x^3+x+1$ (n и k – выбрать самостоятельно).

40. Найти порождающую и проверочную матрицы для циклического кода, заданного следующим порождающим многочленом: $g(x)=x^4+x+1$ (n и k – выбрать самостоятельно).

41. Найти порождающую и проверочную матрицы для циклического кода, заданного следующим порождающим многочленом: $g(x)=x^5+x+1$ (n и k – выбрать самостоятельно).

42. Найти порождающую и проверочную матрицы для циклического кода, заданного следующим порождающим многочленом: $g(x)=x^4+x^3+x+1$ (n и k – выбрать самостоятельно).

43. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, созданного при помощи порождающей матрицы:

$$G_{(7,4)}=\left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

44. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, созданного при помощи порождающей матрицы:

$$G_{(7,4)} = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

45. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, созданного при помощи порождающей матрицы:

$$G_{(8,4)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

46. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, созданного при помощи порождающей матрицы:

$$G_{(7,4)} = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

47. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, созданного при помощи порождающей матрицы:

$$G_{(9,5)} = \left[\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right]$$

48. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, созданного при помощи порождающей матрицы:

$$G_{(7,2)} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

49. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, созданного при помощи порождающей матрицы:

$$G_{(9,2)} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

50. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, если проверочная матрица имеет вид:

$$H_{(7,4)} = \left[\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

51. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, если проверочная матрица имеет вид:

$$H_{(9,5)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

52. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, если проверочная матрица имеет вид:

$$H_{(9,5)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

53. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, если проверочная матрица имеет вид:

$$H_{(9,5)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

54. Построить таблицу синдромов и найти минимальное кодовое расстояние для кода, если проверочная матрица имеет вид:

$$H_{(7,4)} = \left[\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

55. Зашифровать с помощью шифра Виженера с ключом K сообщение M из алфавита мощностью |X|. M = {5, 11, 10, 2, 6, 4, 13, 7, 12}, K = {14, 3, 8, 12}, |X| = 15.

56. Зашифровать с помощью шифра Виженера с ключом K сообщение M из алфавита мощностью |X|. M = {5, 11, 19, 2, 6, 4, 13, 7, 12, 18}, K = {14, 5, 16}, |X| = 21.

57. Зашифровать с помощью шифра Виженера с ключом K сообщение M из алфавита мощностью |X|. M = {5, 11, 1, 2, 6, 4, 13, 10}, K = {1, 5, 10}, |X| = 14.

58. Зашифровать с помощью шифра Виженера с ключом K сообщение M из алфавита мощностью |X|. M = {3, 11, 9, 17, 6, 13, 7, 12, 8}, K = {14, 7}, |X| = 18.

59. Зашифровать с помощью шифра Виженера с ключом K сообщение M из алфавита мощностью |X|. M = {11, 9, 16, 7, 1, 14, 6, 15, 8}, K = {22, 17, 4, 16, 9}, |X| = 23.

60. Зашифровать с помощью шифра Виженера с ключом K сообщение M из алфавита мощностью |X|. M = {4, 21, 9, 18, 26, 19, 7, 22, 11}, K = {19}, |X| = 27.

61. Зашифровать с помощью шифра Виженера с ключом K сообщение M из алфавита мощностью |X|. M = {14, 8, 16, 7, 21, 11, 9, 15, 8}, K = {2, 17, 12, 19}, |X| = 22.

62. Зашифровать с помощью шифра Виженера с ключом K сообщение M из алфавита мощностью |X|. M = {2, 10, 9, 7, 6, 12, 5}, K = {4, 7, 7, 12, 9, 3, 5, 10, 6}, |X| = 13.
63. Построить LFSR-генератор, заданный многочленом $g(x) = x^5 + x^2 + 1$ и начальным состоянием 110102, и получить последовательность, содержащую 10 бит.
64. Построить LFSR-генератор, заданный многочленом $g(x) = x^4 + x^3 + x^2 + 1$ и начальным состоянием 11102, и получить последовательность, содержащую 10 бит.
65. Построить LFSR-генератор, заданный многочленом $g(x) = x^5 + x^3 + 1$ и начальным состоянием 100102, и получить последовательность, содержащую 10 бит.
66. Построить LFSR-генератор, заданный многочленом $g(x) = x^7 + x^2 + 1$ и начальным состоянием 10101102, и получить последовательность, содержащую 10 бит.
67. Построить LFSR-генератор, заданный многочленом $g(x) = x^6 + x^2 + 1$ и начальным состоянием 1100102, и получить последовательность, содержащую 10 бит.
68. Построить LFSR-генератор, заданный многочленом $g(x) = x^5 + x^2 + x + 1$ и начальным состоянием 010102, и получить последовательность, содержащую 10 бит.
69. Построить LFSR-генератор, заданный многочленом $g(x) = x^6 + x^4 + x^3 + x^2$ и начальным состоянием 1101102, и получить последовательность, содержащую 10 бит.
70. Построить LFSR-генератор, заданный многочленом $g(x) = x^7 + x^5$ и начальным состоянием 11110102, и получить последовательность, содержащую 10 бит.
71. Построить LFSR-генератор, заданный многочленом $g(x) = x^7 + x^6 + x^4 + x^3$ и начальным состоянием 11001002, и получить последовательность, содержащую 10 бит.
72. Построить LFSR-генератор, заданный многочленом $g(x) = x^8 + x^7 + x^6 + x^5$ и начальным состоянием 100110102, и получить последовательность, содержащую 10 бит.
73. Построить LFSR-генератор, заданный многочленом $g(x) = x^8 + x^5 + x^3 + 1$ и начальным состоянием 101010102, и получить последовательность, содержащую 10 бит.
74. С помощью критерия χ^2-Пирсона выяснить, является последовательность {11, 19, 16, 4, 5, 19, 7, 8, 16, 1, 15, 7, 12, 13, 0, 15, 15, 5, 19, 10} равномерно распределённой на отрезке $[0; 20)$ при уровне значимости $\alpha = 0.05$? Критические значения

статистики критерия для уровня значимости $\alpha = 0.05$ и различных степеней свободы r приведены в таблице.

r	1	2	3	4	5	6	7
$S_{кр}$	3.841	5.991	7.815	9.488	11.070	12.592	14.067

75. С помощью критерия χ^2-Пирсона выяснить, является последовательность {15, 2, 14, 14, 6, 12, 4, 3, 6, 1, 11, 14, 5, 11, 1, 11} равномерно распределённой на отрезке [0; 17) при уровне значимости $\alpha = 0.05$? Критические значения статистики критерия для уровня значимости $\alpha = 0.05$ и различных степеней свободы r приведены в таблице.

r	1	2	3	4	5	6	7
$S_{кр}$	3.841	5.991	7.815	9.488	11.070	12.592	14.067

76. С помощью критерия χ^2-Пирсона выяснить, является последовательность {21, 0, 3, 7, 0, 20, 23, 12, 20, 20, 1, 6, 17, 13, 24, 23, 21, 0, 21, 22} равномерно распределённой на отрезке [0; 25) при уровне значимости $\alpha = 0.05$? Критические значения статистики критерия для уровня значимости $\alpha = 0.05$ и различных степеней свободы r приведены в таблице.

r	1	2	3	4	5	6	7
$S_{кр}$	3.841	5.991	7.815	9.488	11.070	12.592	14.067

77. С помощью критерия χ^2-Пирсона выяснить, является последовательность {3, 1, 8, 8, 8, 9, 8, 10, 0, 5, 0, 3, 3, 7, 3, 4, 1, 5, 4, 10} равномерно распределённой на отрезке [0; 12) при уровне значимости $\alpha = 0.05$? Критические значения статистики критерия для уровня значимости $\alpha = 0.05$ и различных степеней свободы r приведены в таблице.

r	1	2	3	4	5	6	7
$S_{кр}$	3.841	5.991	7.815	9.488	11.070	12.592	14.067

78. С помощью критерия χ^2-Пирсона выяснить, является последовательность {5, 15, 15, 12, 3, 3, 7, 0, 8, 15, 3, 12, 7, 15, 4, 7, 13, 4, 3, 0} равномерно распределённой на отрезке [0; 16) при уровне значимости $\alpha = 0.05$? Критические значения статистики критерия для уровня значимости $\alpha = 0.05$ и различных степеней свободы r приведены в таблице.

r	1	2	3	4	5	6	7
$S_{кр}$	3.841	5.991	7.815	9.488	11.070	12.592	14.067

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра теоретической и прикладной информатики

Паспорт
расчетно-графического задания (работы)

по дисциплине «Основы теории информации и криптографии», 5 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты изучить выбранный алгоритм из варианта задания сточки зрения его истории создание, теоретических основ, реализации, актуальности и области применения.

При выполнении расчетно-графического задания (работы) студенты должны согласно варианту изучить выбранный алгоритм, привести историю создания данного метода; определить где используется метод, его назначение; изучить теоретические основы алгоритма и привести код алгоритма; проанализировать достоинства и недостатки метода; придумать тестовый пример, который необходимо просчитать теоретически (вручную).

Обязательные структурные части РГЗ.

История создания данного метода;
Где используется, назначение;
Теоретические основы алгоритма;
Код алгоритма на каком-либо языке (не обязательно реализованный самостоятельно);
Достоинства и недостатки метода;
Тестовый пример, решенный теоретически (вручную);
Отчет
Демонстрация работы программы

Оцениваемые позиции:

Степень проработки исследования истории создания данного метода; назначения; теоретических основ алгоритма;
Полнота приведенных достоинства и недостатки метода;
Качество решенного тестового примера
Качество отчета
Правильность работы программы

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), отсутствует анализ объекта, диагностические признаки не обоснованы, программные средства не выбраны или не соответствуют современным требованиям, оценка составляет от 0 до 9 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, программные средства не соответствуют современным требованиям, оценка составляет от 10 до 13 баллов.
- Работа считается выполненной **на базовом** уровне, если анализ объекта выполнен в

полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны ,но не оптимизированы, программные средства выбраны без достаточного обоснования, оценка составляет от 14до 17 баллов.

- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны и оптимизированы, выбор программных средств обоснован, оценка составляет от 17 до 20 баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Примерный перечень тем РГЗ(Р)

Тема	Подтема	Алгоритм
Экономное кодирование		Арифметическое кодирование
	Словарные методы кодирования	Метод Зива-Лемпела LZ-метод
		LZ77
		LZSS
		LZ78
		LZW
	Адаптивные алгоритмы кодирования	Адаптивный алгоритм арифметического кодирование
		Адаптивный алгоритм кодирования Хаффмана
Генераторы псевдослучайных последовательностей	На основе односторонних функций	ANSI X9.17
		FIPS-186
		Yarrow-160
	На основе проблем теории чисел	RSA-алгоритм генерации псевдослучайных последовательностей
		Модификация Микали - Шнорра RSA-алгоритм генерации псевдослучайных последовательностей
		BBS (Blum–Blum–Shub)
Криптоалгоритмы	Алгоритмов шифрования, основанных на вычисление в поле Галуа	RIJNDAEL (AES)
		A5/1
Факторизация целых чисел	Методы с субэкспоненциальной сложностью	Алгоритм Диксона.
		Алгоритм Бриллхарта – Моррисона
		Квадратичное решето
		Методы Шнорра—Ленстры
		Ленстры—Померанса
		Алгоритм решета числового поля для факторизации целых чисел специального вида (SNFS)
		Алгоритм решета числового поля для факторизации произвольных целых чисел (GNFS)