ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет прикладной математики и информатики

“УТВЕРЖДАЮ”

Декан ФПМИ

профессор, д.т.н. Лемешко Борис Юрьевич

“___ ”_____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплины специализаций: Основы теории информации и криптографии

ООП: специальность 010503.65 Математическое обеспечение и администрирование информационных систем

Шифр по учебному плану: ДС.Ф.1.4

Факультет: прикладной математики и информатики очная форма обучения

Курс: 3, семестр: 5

Лекции: 18

Практические работы: - Лабораторные работы: 18

Курсовой проект: - Курсовая работа: - РГЗ: 5

Самостоятельная работа: 59

Экзамен: - Зачет: 5

Всего: 95

Новосибирск

2011

Рабочая программа составлена на основании _Государственного образовательного стандарта высшего профессионального образования по направлению (специальности): 351500 Математическое обеспечение и администрирование информа-ционных систем.(№ 72 мжд/сп от 10.03.2000)

ДС.Ф.1.4, дисциплины федерального компонента

Рабочая программа обсуждена на заседании кафедры Программных систем и баз данных протокол № 3 от 31.08.2011

Программу разработал

ассистент, Гультяева Татьяна Александровна

Заведующий кафедрой

профессор, д.т.н. Попов Александр Александрович

Ответственный за основную образовательную программу

профессор, д.т.н. Попов Александр Александрович

1. Внешние требования

Таблица 1.1

Шифр дисциплины	Содержание учебной дисциплины	Часы
ДС.Ф.1.4	Концептуальная записка по специальности 010503.65 - "Математическое обеспечение и администрирование информационных систем". Вероятностно - статистические модели сообщений и их свойства. Основы экономного кодирования. Алгоритмы побуквенного кодирования информации. Основные математические модели элементарных криптосистем. Основы помехоустойчивого кодирования. Основы криптографии. Основные положения теории чисел. Алгоритмы генерации псевдослучайных последовательностей. Методы тестирования чисел на простоту. Методы решения сравнений. Методы решения задачи дискретного логарифма. Алгоритмы факторизации.	**95**

2. Особенности (принципы) построения дисциплины

Таблица 2.1

Особенности (принципы) построения дисциплины

Особенность (принцип)	Содержание
Основания для введения дисциплины в учебный план по направлению или специальности	Решение Ученого совета ФПМИ протокол №3 от 23.04.2007.
Адресат курса	Студенты специальности 010503.65 - "Математическое обеспечение и администрирование информационных систем".
Основная цель (цели) дисциплины	Изучив дисциплину, вы научитесь решать теоретические задачи по основам теории информации, реализовывать, применять и анализировать основные компьютерные методы криптологии.
Ядро дисциплины	Вероятностно - статистические модели сообщений и их свойства; Основы экономного кодирования; Основы помехоустойчивого кодирования; Теоретические и практические основы криптографии; Основы теории чисел.
Связи с другими учебными дисциплинами основной образовательной программы	Дискретная математика Теории вероятности Общая алгебра Методы программирования.
Требования к первоначальному уровню подготовки обучающихся	Для успешного изучения курса студенту необходимо владеть знаниями дискретной математики, основ теории вероятности, общей алгебры, методов программирования.
Особенности организации	

учебного процесса по дисциплине	

3. Цели учебной дисциплины

Таблица 3.1

После изучения дисциплины студент будет

иметь представление	
1	о вероятностно - статистических моделях сообщений и их свойства
2	об основах экономного кодирования
3	об основах помехоустойчивого кодирования
4	о теоретических и практических основах криптографии
5	об основах теории чисел
знать	
6	свойства вероятно-статистических моделях сообщений
7	алгоритмы побуквенного кодирования информации
8	алгоритмы помехоустойчивого кодирования информации
9	основные математические модели элементарных криптосистем
10	алгоритмы генерации псевдослучайных последовательностей
11	методы тестирования чисел на простоту
12	методы решения сравнений
13	методы решения задачи дискретного логарифма
14	алгоритмы факторизации
уметь	
15	рассчитывать основные теоретические показатели моделей сообщений
16	разрабатывать программные приложения для решения поставленных задач
иметь опыт (владеть)	
17	реализовывать алгоритмы, необходимые для решения поставленных задач

4. Содержание и структура учебной дисциплины

Лекционные занятия

Таблица 4.1

(Модуль), дидактическая единица, тема	Часы	Ссылки на цели
Семестр: 5		
Модуль: Основные аспекты		
Дидактическая единица: Основные аспекты теории информации (Вероятностно - статистические модели сообщений и их свойства)		
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.	4	1, 15, 6

Избыточность. Количество информации по К. Шеннону и его свойства.		
Модуль: Кодирование		
Дидактическая единица: Основные принципы кодирования (Основы экономного кодирования. , Алгоритмы побуквенного кодирования информации, Основы помехоустойчивого кодирования.)		
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.	2	2, 7
Тема 3. Помехоустойчивое кодирование. Коды с обнаружением ошибок. Коды с исправлением ошибок. Линейные блоковые коды. Коды Хэмминга. Циклические коды.	2	3, 8
Модуль: Криптография		
Дидактическая единица: Основы криптографии (Основные математические модели элементарных криптосистем, Основы криптографии.)		
Тема 4. Основы криптографии. Терминология и основные понятия криптологии. Основные аспекты криптографии. Основные аспекты криптоанализа. Шеноновские модели криптографии. Теоретико-информационные оценки стойкости симметричных криптосистем.	2	4, 9
Модуль: Криптология		
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.)		
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	2	10, 4

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	2	11, 4, 5
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.	2	12, 4, 5
Тема 8. Разложение на множители (факторизация) Метод Ферма. Ро- факторизация Полларда. Метод Ро-Полларда. Метод Шермана-Лемана. Метод Ленстры.	1	11, 4, 5
Тема 8. Примеры систем шифрования, основанные на проблемах теории чисел Система шифрования RSA. Система шифрования Диффи-Хеллмана.	1	4

Лабораторная работа Таблица 4.2

(Модуль), дидактическая единица, тема	**Учебная деятельность**	**Часы**	**Ссылки на цели**
Семестр: 5			
Модуль: Основные аспекты			
Дидактическая единица: Основные аспекты теории информации (Вероятностно - статистические модели сообщений и их свойства)			
Решение типовых задач по теме "Основные аспекты теории информации"	Приобретение навыка решения практических задач, отражающих основные свойства источников дискретных	4	1, 15, 16, 6

	сообщений (ИДС).		
Модуль: Кодирование			
Дидактическая единица: Основные принципы кодирования (Основы экономного кодирования. , Алгоритмы побуквенного кодирования информации, Основы помехоустойчивого кодирования.)			
Основные методы побуквенного кодирования	Освоение основных алгоритмов побуквенного кодирования. Приобретение навыка реализации одного из алгоритмов побуквенного кодирования (согласно варианту).	3	16, 17, 2, 7
Помехоустойчивое кодирование	Освоение основных алгоритмов помехоустойчивого кодирования. Приобретение навыка реализации алгоритма обнаружения ошибок (контроль четности) и исправления ошибок (алгоритм Хэмминга).	2	16, 17, 3, 8
Модуль: Криптография			
Дидактическая единица: Основы криптографии (Основные математические модели элементарных криптосистем, Основы криптографии.)			
Шифры перестановки и замены	Освоение основных алгоритмов шифрования перестановки и замены. Приобретение навыка реализации одного из алгоритмов шифрования перестановкой и заменой (согласно варианту).	2	16, 4, 9
Модуль: Криптология			
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.)			
Генерирование равномерно распределенных псевдослучайных последовательностей	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.	2	10, 16, 17, 4
Тестирование чисел на простоту и построение больших простых чисел	Освоение основных программных методов тестирования чисел на простоту. Приобретение навыка реализации одного из алгоритмов тестирования чисел на простоту (согласно варианту).	2	11, 12, 16, 17, 5
Факторизация составного числа	Освоение простых алгоритмов факторизации составного числа. Приобретение навыка реализации одного из алгоритмов факторизации составного числа (согласно варианту).	3	12, 14, 16, 17, 5

5. Самостоятельная работа студентов

Семестр- 5, Подготовка к зачету

Подготовка к зачету занимает 6 часов. Подготовка к зачету заключается в изучении материала курса по конспекту лекций (см. п. 7) и рекомендованной литературе (см. п. 7).

Семестр- 5, РГЗ

Работа над РГЗ занимает 5 часов. Задание на РГЗ см. в п. 8.1.

Семестр- 5, Подготовка к занятиям

Лабораторные работы проводятся с целью формирования практических навыков реализации и анализа компьютерных методов криптологии. Выполнение лабораторных работ предполагает знание студентами лекционного материала, изучения дополнительной информации (рекомендуемая литература, самостоятельный поиск источников). Лабораторные работы проводятся в терминальных классах на базе ПК IBM/PC. В часы, отведенные для самостоятельной работы (САР) , студенты приобретают теоретические знания и практические навыки, необходимые им для выполнения лабораторных работ. Ряд тем курса студенты осваивают самостоятельно, пользуясь методическими пособиями и материалами лекций (или их фрагментов). К ним относятся темы 5,6,8 (частично).

Подготовка к лекциям занимает 27 часов. Подготовка к лекциям заключается в изучении материалов предыдущей лекции ознакомлению с материалом текущей лекции по конспекту лекций (см. п. 7).

Подготовка к лабораторным работам занимает 21 часов. Подготовка к лабораторным работам заключается в изучении методических указаний к лабораторным работам (см. п. 8.1).

6. Правила аттестации студентов по учебной дисциплине

Виды образовательных траекторий

«min» – соответствует самому слабому студенту, который может быть допущен до экзамена/зачёта.

«норм» – соответствует студенту, получающему оценку «A–», т.е. 90 баллов в 100-балльной шкале.

Лабораторные работы

По дисциплине предусмотрено 5 лабораторных работ.

Общее количество баллов за все лабораторные работы (*LR*) вычисляется по формуле:

$$LR = \sum_{i=1}^{5} LR_i,$$

где LR_i – суммарный балл за *i*-ую лабораторную работу.

Баллы за каждую лабораторную работу (LR_i) начисляются по формуле:

$$LR_i = FMade_i + QMade_i + TMade_i + FDefence_i + QDefence_i + TDefence_i,$$

где i – номер лабораторной работы,
$FMade_i$ – балл за факт выполнения лабораторной работы,
$QMade_i$ – балл за качество выполнения лабораторной работы,
$TMade_i$ – балл за срок выполнения лабораторной работы,
$FDefence_i$ – балл за факт защиты лабораторной работы,
$QDefence_i$ – балл за качество защиты лабораторной работы,
$TDefence_i$ – балл за срок защиты лабораторной работы.

Баллы за факт выполнения ($FMade_i$) и защиты ($FDefence_i$) лабораторной работы начисляются в зависимости от коэффициента сложности выполнения или защиты работы (конкретные значения приведены ниже).

Баллы за качество выполнения ($QMade_i$) и защиты ($QDefence_i$) лабораторной работы начисляются согласно критериям оценивания, приведённым в описании задания на лабораторную работу.

Предполагается, что студент с образовательной траекторией «min» набирает 0 баллов за качество выполнения каждой лабораторной работы и по 1 баллу за качество защиты каждой лабораторной работы.

Предполагается, что студент с образовательной траекторией «норм» на защите лабораторной работы правильно выполняет все возможные задания, т.е. набирает максимально возможный балл за качество защиты.

Баллы за срок выполнения ($TMade_i$) и защиты ($TDefence_i$) лабораторной работы начисляются по формулам:

$$TMade_i = \max\{0; 18 - WeekMade_i\} \quad \text{и} \quad TDefence_i = \max\{0; 18 - WeekDefence_i\},$$

где i – номер лабораторной работы,
$WeekMade_i$ – номер недели, на которой была сдана лабораторная работа,
$WeekDefence_i$ – номер недели, на которой была защищена лабораторная работа.

Предполагается, что студент с образовательной траекторией «min» сдаёт и защищает все лабораторные работы на 16 неделе.

Таблица начисления баллов студенту с образовательной траекторией «min»:

№ л.р.	коэф.	Выполнение	коэф.	Защита	Всего

	слож-ности	Факт		Кач.	Срок		слож-ности	Факт		Кач.	Срок		за л.р.
		есть	Балл	Балл	Нед	Балл		есть	Балл	Балл	Нед	Балл	
1	***10,0***	***1***	**74**	***0,0***	***16***	**2**	***1,0***	***1***	**7**	***1,0***	***16***	**2**	**86,0**
2	***8,0***	***1***	**59**	***0,0***	***16***	**2**	***1,0***	***1***	**7**	***1,0***	***16***	**2**	**71,0**
3	***10,0***	***1***	**74**	***0,0***	***16***	**2**	***2,0***	***1***	**15**	***1,0***	***16***	**2**	**94,0**
4	***6,0***	***1***	**44**	***0,0***	***16***	**2**	***1,0***	***1***	**7**	***1,0***	***16***	**2**	**56,0**
5	***8,0***	***1***	**59**	***0,0***	***16***	**2**	***1,0***	***1***	**7**	***1,0***	***16***	**2**	**71,0**
Всего:	42,0		**310**	**0,0**		**10,0**	6,0		**43**	**5,0**		**10,0**	**378,0**

Таблица начисления баллов студенту с образовательной траекторией «норм»:

№ л.р.	коэф. слож-ности	Выполнение					коэф. слож-ности	Защита					Всего за л.р.
		Факт		Кач.	Срок			Факт		Кач.	Срок		
		есть	Балл	Балл	Нед	Балл		есть	Балл	Балл	Нед	Балл	
1	***10,0***	***1***	**74**	***8,0***	***3***	**15**	***1,0***	***1***	**7**	***1,0***	***3***	**15**	**120,0**
2	***8,0***	***1***	**59**	***8,0***	***6***	**12**	***1,0***	***1***	**7**	***1,0***	***6***	**12**	**99,0**
3	***10,0***	***1***	**74**	***8,0***	***9***	**9**	***2,0***	***1***	**15**	***1,0***	***9***	**9**	**116,0**
4	***6,0***	***1***	**44**	***8,0***	***12***	**6**	***1,0***	***1***	**7**	***1,0***	***12***	**6**	**72,0**
5	***8,0***	***1***	**59**	***8,0***	***15***	**3**	***1,0***	***1***	**7**	***1,0***	***15***	**3**	**81,0**
Всего:	42,0		**310**	**40,0**		**45,0**	6,0		**43**	**5,0**		**45,0**	**488,0**

Итого за лабораторные работы: «min»=378 балла, «норм»=488 баллов.

Лекции

По дисциплине предусмотрено 8 лекций.

Общее количество баллов за посещение лекций (*Lec*) вычисляется по формуле:

$$Lec = 1 \cdot Visit,$$

где *Visit* – количество посещённых студентом лекций.

Предполагается, что студент с образовательной траекторией «min» не посещает лекции, а студент с образовательной траекторией «норм» пропустит 2 лекции, т.е. посетит 6 лекций.

Итого за лекции: «min»=0 баллов, «норм»= 6 баллов.

Билет на зачете

Билет состоит из 3 заданий (1 задание с весом = 1.5, 2 задания с весом = 0.75). На выполнение заданий билет отводится около 1 часа. Максимальное число баллов за билет (*TicketMax*) равно 30 баллам.

Общее количество баллов за билет (*Ticket*) вычисляется по формуле:

$$Ticket = \sum_{i=1}^{3} Percent_i \cdot Task_i,$$

где $Percent_i$ – величина от 0 до 1, характеризующая полноту выполнения *i*-го задания;

$Task_i$ – максимальный балл за *i*-ое задание билета, рассчитанный в соответствии с весом задания и максимальным числом баллов за билет. При этом, $TicketMax = \sum_{i=1}^{3} Task_i$.

Билет считается сданным, если $Ticket \geq 10$ баллов.

Итого за билет: «min»=10 баллов, «норм»=25 баллов.

Условия проведения экзамена/зачёта

Все баллы за факт выполнения и защиты лабораторных работ, РГР вычисляются из соотношения:

$$Total\ (\min) = K * Total\ (норм)$$

где *K* – доля знаний студента с образовательной траекторией «норм», достаточных для допуска к экзамену/зачёту (число от 0 до 1).

Для данной дисциплины *K*=0,7.

Для допуска к экзамену/зачёту к концу семестра (до экзамена/зачёта) нужно набрать минимальный балл (*DopuskBall*), который вычисляется по формуле:

$$DopuskBall = Total\ (\min) - Exam\ (\min)$$

где *Exam(min)* – минимальный набранный на экзамене балл, при котором экзамен считается сданным.

Для данной дисциплины *DopuskBall* = **378 балл** (в шкале 0–100 — ***47,6 баллов***).

Экзамен/зачёт включает Билет. Чтобы экзамен/зачёт был сдан число баллов за билет должно быть не менее 10. Если экзамен/зачёт не сдан, студент направляется на пересдачу экзамена/зачёта, а набранные в семестре баллы устанавливаются равными минимальному баллу, необходимому для допуска к экзамену/зачёту, т.е. равными *DopuskBall*.

Вычисление рейтинга по дисциплине

Рейтинг по дисциплине (*Total*) вычисляется по формуле:

$$Total = LR + Lec + Ticket.$$

Total(min) = 388 ~ 50 баллам по 100-балльной шкале.
Total(норм) = 555 ~ 90 баллам по 100-балльной шкале.
Формула перевода рейтинга в 100-балльную шкалу (*Ball100*):

$$Ball\,100 = \min\{100;\ \max\{0;\ Total \cdot a + b\}\},$$

$$a = \frac{90 - 50}{Total\ (норм) - Total\ (\min)} \quad \text{и} \quad b = 50 - Total\ (\min) \cdot a.$$

a = 0.2395, b = -42.93.

Таблица соответствия «буквенных» оценок и балльной шкалы 0–100.

Буква	Балл (0-100)	Буква	Балл (0-100)	Буква	Балл (0-100)	Буква	Балл (0-100)	Буква	Балл (0-100)
A+	[97; 100)	B+	[87; 90)	C+	[77; 80)	D+	[67; 70)	E	[50; 60)
A	[93; 97)	B	[83; 87)	C	[73; 77)	D	[63; 67)		
A-	[90; 93)	B-	[80; 83)	C-	[70; 73)	D-	[60; 63)		

Оценки за контрольные недели

Общие принципы расчёта границ интервалов для оценок «2», «1» и «0»:

Оценка «2»:

- срок выполнения и защиты берётся равным сроку для «норм» + 1 неделя;

- качество выполнения и защиты берётся равным качеству для «норм».

Оценка «1»:

- срок выполнения и защиты берётся равным сроку для «норм» + 2 недели;
- качество выполнения берётся равным половине качества для «норм»;
- качество защиты берётся равным качеству для «min».

Суммируются только те виды работ, которые успевают выполниться до 7 (13) недели включительно.

В соответствие с набранными к концу каждой контрольной недели баллами выставляется оценка за контрольные недели по следующему правилу:

I контрольная неделя:

$$\begin{aligned} &Total \in [217 ; \infty) \Rightarrow \text{"2"}, \\ &Total \in [118 ; 217) \Rightarrow \text{"1"}, \\ &\textit{иначе} \Rightarrow \text{"0"}. \end{aligned}$$

II контрольная неделя:

$$\begin{aligned} &Total \in [403 ; \infty) \Rightarrow \text{"2"}, \\ &Total \in [327 ; 403) \Rightarrow \text{"1"}, \\ &\textit{иначе} \Rightarrow \text{"0"}. \end{aligned}$$

7. Список литературы

7.1 Основная литература

В печатном виде

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.
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. - Рекомендовано УМО.

В электронном виде

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

7.2 Дополнительная литература

В печатном виде

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

В электронном виде

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

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

В печатном виде

1. 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.
2. 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.

В электронном виде

1. 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.
2. 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
3. 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

8.2 Программное обеспечение

1. Microsoft, Office XP, Офисный пакет приложений
2. Microsoft, eMbedded Visual C++, Интегрированная среда разработки
3. Maple, Maple 12: , Среда для решения математических, инженерно-технических и научных задач Maple

9. Контролирующие материалы для аттестации студентов по дисциплине

В качестве контролирующих материалов используются вопросы к лабораторным работам из методических указаний, тестовые задания по курсу, вопросы по всему материалу курса.

Примерные тестовые задания по курсу
"Основы теории информации и криптографии"(промежуточный контроль)

Энтропия ИДС это	▪ Количественная мера априорной неосведомленности о том, какое из сообщений будет порождено источником ▪ Количественная мера апостериорной осведомленности о том, какое из сообщений будет порождено источником ▪ Среднее количество собственной информации Среднее количество взаимной информации
В системах сжатия без потерь информации	▪ Декодер восстанавливает данные источника абсолютно без потерь ▪ Есть блок квантователя ▪ Вводит понятие меры среднеквадратичного различия между сообщениями исходным сообщением и полученным в результате декодирования. ▪ Существует взаимно однозначное соответствие между исходным сообщением и полученным в результате декодирования ▪ Должно обеспечиваться кодирование наиболее экономным образом

Перечень вопросов к защите лабораторных работ по курсу
"Основы теории информации и криптографии"(промежуточный контроль)

1. Доказать следующее свойство функционала энтропии:
$H(\xi) \geq 0$
2. $H(\xi) = 0$, если ξ неслучайно.
3. Доказать свойство аддитивность функционала энтропии.
4. Доказать, что если к алфавиту символов добавить символ с нулевой вероятностью, то энтропия ИДС не изменится.
5. Доказать свойство иерархической аддитивности функционала энтропии:
$H(X_1, X_2, \ldots, X_n) = H(X_1) + H(X_2 \mid X_1) + \ldots + H(X_n \mid X_1, X_2, \ldots, X_n)$
6. Доказать свойство симметрии функционала средней взаимной информации.
7. Доказать, что $0 \leq \hat{I}(X, Y) \leq \min(H(X), H(Y))$
8. Доказать, что равенство нулю в неравенстве $0 \leq \hat{I}(X, Y) \leq \min(H(X), H(Y))$ возможно тогда и только тогда, когда X, Y статистически независимы.
9. Доказать, что $\hat{I}(X, (Y_1, Y_2)) = \hat{I}(X, Y_1) + \hat{I}(X, Y_2)$, если Y_1, Y_2 независимы.
10. Алгоритм Хаффмана.
11. Алгоритм Шеннона.
12. Алгоритм Шеннона-Фано.
13. Алгоритм Гильбера-Мура.
14. Алгоритм перевода дробных чисел в двоичную систему счисления.
15. Сжатие без потерь информации.
16. Сжатие с потерей информации.
17. Теорема Шеннона. (о кодировании в дискретных каналах без шума)
18. Оптимальное побуквенное кодирование.
19. Неравенство Крафта.
20. Помехоустойчивое кодирование. Теорема Шеннона (о кодировании в дискретных каналах с шумом)..
21. Коды с обнаружением ошибок.
22. Коды с исправлением ошибок.

23. Построение таблицы синдромов. С какой целью это делается?
24. Алгоритм перевода дробных чисел в двоичную систему счисления.
25. Найти порождающую и проверочные матрицы для циклического кода, заданного следующим порождающим многочленом:

    a. $g(x) = x^2 + x + 1$

    b. $g(x) = x^3 + x + 1$

    c. $g(x) = x^4 + x + 1$

    d. $g(x) = x^5 + x^2 + 1$

    e. $g(x) = x^6 + x + 1$

    f. $g(x) = x^7 + x + 1$

    g. $g(x) = x^7 + x^3 + 1$

    h. $g(x) = x^8 + x^4 + x^3 + x^2 + 1$

    i. $g(x) = x^9 + x^4 + 1$

    j. $g(x) = x^{10} + x^3 + 1$

    k. $g(x) = x^{11} + x^2 + 1$

    l. $g(x) = x^{12} + x^6 + x^4 + x + 1$

    m. $g(x) = x^{13} + x^4 + x^3 + x + 1$

    n. $g(x) = x^{14} + x^5 + x^3 + x + 1$

    o. $g(x) = x^{15} + x + 1$

При этом пару (n, k) подобрать самостоятельно. Проверить основные свойства линейных кодов, свойство линейности полученных кодов.

26. Основные понятия криптографии.
27. Протоколы обмена ключами.
28. Основные аспекты криптоанализа.
29. Общая схема симметричных криптосистем.
30. Математические модели элементарных криптосистем.
31. Криптостойкость симметричных криптосистем.
32. Пессимистическое утверждение Шеннона (теорема).
33. Показатели криптостойкости.
34. Требования, предъявляемые к современным криптографическим системам.
35. Теорема Эйлера
36. Теорема Ферма (малая теорема Ферма или малая теорема Эйлера).
37. С какой целью в криптологии используют псевдослучайные последовательности?
38. Зачем генерировать псевдослучайные последовательности с максимальным периодом?
39. Равномерно распределенная случайная последовательность.
40. Классификация алгоритмов генерации псевдослучайных последовательностей.
41. Конгруэнтные генераторы.
42. Рекуренты в конечном поле.
43. Криптостойкие генераторы на основе односторонних функций.
44. Криптостойкие генераторы, основанные на проблемах теории чисел.
45. Методы «улучшения» элементарных псевдослучайных последовательностей.
46. Комбинирование LFSR-генераторов.
47. Построить LFSR-генератор, заданный одним из следующих примитивным многочленом:

    a. $g(x) = x^8 + x^4 + x^3 + x^2 + 1$

    b. $g(x) = x^9 + x^4 + 1$

c. $g(x) = x^{10} + x^3 + 1$

d. $g(x) = x^{11} + x^2 + 1$

e. $g(x) = x^{12} + x^6 + x^4 + x + 1$

f. $g(x) = x^{13} + x^4 + x^3 + x + 1$

g. $g(x) = x^{14} + x^5 + x^3 + x + 1$

h. $g(x) = x^{15} + x + 1$

i. $g(x) = x^{16} + x^5 + x^3 + x^2 + 1$

j. $g(x) = x^{17} + x^3 + 1$

k. $g(x) = x^{17} + x^5 + 1$

l. $g(x) = x^{17} + x^6 + 1$

m. $g(x) = x^{18} + x^7 + 1$

n. $g(x) = x^{18} + x^5 + x^2 + x + 1$

o. $g(x) = x^{19} + x^5 + x^2 + x + 1$

48. Простые числа.
49. Метод пробных делений
50. Решето Эратосфена
51. Критерий Вильсона
52. Тест на основе малой теоремы Ферма
53. Тест Соловея – Штрассена
54. Тест Леманна.
55. Тест Рабина – Миллера
56. Полиномиальный тест распознавания простоты.
57. Тест Конягина – Померанса.
58. Метод Михалеску.
59. Решить сравнение первой степени используя:
    a. Алгоритм Евклида;
    b. Расширенный алгоритм Евклида;
    c. Метод Эйлера (если возможно).

    Сравнения:

    A. $5x \equiv 26 \pmod{12}$

    B. $5x \equiv 3 \pmod{12}$;

    C. $256x \equiv 179 \pmod{337}$

    D. $1215x \equiv 560 \pmod{2755}$

    E. $1296x \equiv 1105 \pmod{2413}$

    F. $115x \equiv 85 \pmod{335}$

Привести все шаги алгоритма. Поверить результат (подставить найденное решение в сравнение).

60. Метод факторизации Ферма.
61. Метод факторизации ρ -Полларда.
62. $(p-1)$ - факторизация Полларда.
63. Метод Шермана-Лемана.
64. Метод Ленстры.
65. Найти все первообразные корни, меньше m :
    a. $m = 5$
    b. $m = 7$
    c. $m = 11$

d. $m = 13$
e. $m = 17$
f. $m = 19$
g. $m = 23$
h. $m = 29$
i. $m = 31$
i. $m = 37$
k. $m = 41$
l. $m = 43$
m. $m = 47$
n. $m = 53$
o. $m = 57$
p. $m = 59$

Перечень вопросов по курсу "Основы теории информации и криптографии"(итоговый контроль)

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

Перечень примерных вопросов по курсу "Основы теории информации и криптографии"(остаточный контроль)

1. Задачи, решаемые в теории информации	▪ Кодирование дискретных источников ▪ Кодирование информации для передачи по каналу с шумом ▪ Кодирование с заданным критерием качества ▪ Кодирование информации для системы со многими пользователями ▪ Секретная связь, системы защиты информации от несанкционированного доступа
2. ИДС – это	▪ Источник дискретного сообщения ▪ Источник дискретный случайный ▪ Источник дальнего сигнала
3. Алфавит источника непрерывного сообщения	▪ Имеет конечную мощность ▪ Это счетное множество ▪ Имеет бесконечную мощность
4. Построить LFSR-генератор, заданный примитивным многочленом: $g(x) = x^9 + x^4 + 1$	