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
# **Программные средства защиты информации**

Образовательная программа: 02.04.03 Математическое обеспечение и администрирование информационных систем, магистерская программа: Математическое и программное обеспечение информационных технологий

Курс: 2, семестр : 3

Факультет прикладной математики и информатики,

| | | **Семестр** |
|---|---|---|
| **№** | **Вид деятельности** | **3** |
| **1** | Всего зачетных единиц (кредитов) | 3 |
| **2** | Всего часов | 108 |
| **3** | Всего занятий в контактной форме, час. | 68 |
| **4** | Лекции, час. | 18 |
| **5** | Практические занятия, час. | 0 |
| **6** | Лабораторные занятия, час. | 36 |
| **7** | из них в активной и интерактивной форме, час. | 0 |
| **8** | Аттестация, час. | 2 |
| **9** | Консультации, час. | 12 |
| **10** | Самостоятельная работа, час. | 40 |
| **11** | Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе) | |
| **12** | Вид аттестации | Э |

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 02.04.03 Математическое обеспечение и администрирование информационных систем

ФГОС введен в действие приказом №1416 от 30.10.2014 г. , дата утверждения: 26.11.2014 г.

Место дисциплины в структуре учебного плана: Блок 1, базовая

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 02.04.03 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.10 владение навыками использования основных моделей информационных технологий и способов их применения для решения задач в предметных областях; *в части следующих результатов обучения*:** |
| у7. Уметь определять комплекс превентивных мер по защите конфиденциальных данных |
| ***Компетенция ФГОС*: ОПК.11 владение навыками выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования; *в части следующих результатов обучения*:** |
| у1. Уметь формулировать на основе категорий информационной безопасности требования к разрабатываемым средствам защиты информации |
| ***Компетенция ФГОС*: ОПК.4 владение теоретическими основами информатики как науки; знание проблем современной информатики, ее категории и связи с другими научными дисциплинами, понимание основных этапов и тенденции развития программирования, математического обеспечения и информационных, технологий; *в части следующих результатов обучения*:** |
| з1. Знать встроенные средства защиты информации |
| з5. Знать основные методики создания политики безопасности предприятия с учетом основных рисков информационных атак |
| ***Компетенция ФГОС*: ПК.1 владение навыками применения математических основ информатики при разработке и исследовании нового программного обеспечения; *в части следующих результатов обучения*:** |
| у1. Уметь реализовывать алгоритмы шифрования |

## 2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

| **Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)** | **Формы организации занятий** |
|---|---|
| *Программные средства защиты информации* | |
| **ПК.1.у1 Уметь реализовывать алгоритмы шифрования** | |
| **1**.Основные симметричные и асимметричные криптоалгоритмы, потоковые и блочные шифры, симметричные и асимметричные криптосистемы | Лекции; Лабораторные работы; Самостоятельная работа |
| **2**.Реализовывать и анализировать потоковые криптографические шифры | Лабораторные работы; Самостоятельная работа |
| **3**.Реализовывать и анализировать симметричные и асимметричные криптографические шифры | Лабораторные работы; Самостоятельная работа |
| **4**.реализовывать симметричные алгоритмы шифрования | Лабораторные работы; Самостоятельная работа |
| **5**.реализовывать асимметричные алгоритмы шифрования | Лабораторные работы; Самостоятельная работа |
| **ОПК.4.з1 Знать встроенные средства защиты информации** | |
| **6**.встроенные средства защиты информации | Лекции; Лабораторные работы |
| **ОПК.4.з5 Знать основные методики создания политики безопасности предприятия с учетом основных рисков информационных атак** | |
| **7**.Основные методики создания политики безопасности предприятия с учетом основных рисков информационных атак | Лекции; Самостоятельная работа |
| **8**.Формулировать на основе категорий информационной безопасности требования к разрабатываемым средствам защиты информации | Лекции; Самостоятельная работа |
| **ОПК.10.у7 Уметь определять комплекс превентивных мер по защите конфиденциальных данных** | |
| **9**.О реализации и оптимизации криптографических алгоритмов с контролем правильности реализации | Лекции; Самостоятельная работа |

| | |
|---|---|
| **10**.Отечественные и зарубежные стандарты и рекомендации, представляющие общие подходы к обеспечению безопасности | Лекции; Самостоятельная работа |
| **11**.Определять комплекс превентивных мер по защите конфиденциальных данных | Лекции; Самостоятельная работа |
| **ОПК.11.у1 Уметь формулировать на основе категорий информационной безопасности требования к разрабатываемым средствам защиты информации** | |
| **12**.О принципы проектирования программ защиты информации с учетом необходимого уровня надежности | Лекции; Самостоятельная работа |
| **13**.О соблюдении правовых аспектов разработки и использовании программных средств защиты информации | Лекции; Самостоятельная работа |
| **14**.основные средства защиты информации: шифрование, контроль целостости, хэширование | 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: 3** | | | | |
| **Дидактическая единица: Общие понятия предмета** | | | | |
| 1. Нарушения, механизмы и службы защиты | 0 | 2 | 11, 14, 6, 7, 8 | Изучение вопросов о том, что такое криптология, криптография, открытый текст, шифрование, ключ, криптоанализ. Типы криптоанализа. 2 критерия защищённости схемы шифрования. Изучение вопросов о том, что такое Что такое защита информации, информационная безопасность, доступность, целостность, конфиденциальность, что такое абсолютно стойкий шифр, Необходимые и достаточные условия абсолютной стойкости шифра.Изучение что такое лавинный эффект, диффузия и конфузия. |

| | | | | |
|---|---|---|---|---|
| 2. Основные понятия криптологии | 0 | 2 | 14 | Изучение вопросов о том, что такое защита информации, информационная безопасность, что такое доступность, целостность, конфиденциальность; что такое идентификация, аутентификация, что представляет собой сервис безопасности "контроль целостности", что представляют собой сервисы безопасности "анализ защищённости" и "обеспечение отказоустойчивости", что представляет собой сервис безопасности "обеспечение обслуживаемости", что представляет собой сервис безопасности "туннелирование", что представляет собой сервис безопасности "управление доступом", в чём заключается суть ролевого управления доступом, Что представляют собой такие сервисы безопасности, как "протоколирование" и "аудит", что представляет собой сервис безопасности "экранирование"? Изучение 3х аспекта защиты информации, 4 группы активных атак. Модель защиты сети. Характеристики, на основе которых строится классификация криптографических систем. 4 вида нарушений защиты (атак). Пассивные и активные атаки. |
| **Дидактическая единица: Шифрование с 1 ключом** | | | | |
| 3. Симметричное шифрование | 0 | 3 | 1, 8, 9 | Изучение схемы симметричной криптосистемы. Преимущества и недостатки использования однократного гаммирования. Алгоритмы шифрования AES,ГОСТ, DES. Блочные режимы шифрования. Сеть Фейстеля. |
| **Дидактическая единица: Шифрование с 2 ключами** | | | | |

| | | | | |
|---|---|---|---|---|
| 4. Введение в теорию чисел | 0 | 2 | 1, 12 | Изучение основ теории чисел. Определение и свойства функции Эйлера. Малая теорема Ферма. Теорема Эйлера. Схема Диффи-Хеллмана. Схема асимметричной криптосистемы. Алгоритм Евклида. Сравнения первой степени. |
| 5. Ассиметричное шифрование | 0 | 3 | 1, 10, 12, 6, 8 | Изучение достоинств и недостатков асимметричных криптоалгоритмов. Схема асимметричной криптосистемы. Алгоритм шифрования RSA.Схема обмена ключами Диффи-Хеллмана. Распределение открытых ключей в асимметричной криптосистеме. Распределение секретных ключей в асимметричной криптосистеме. |
| **Дидактическая единица: Целостность** | | | | |
| 6. Контроль целостности | 0 | 2 | 10, 12, 13, 6, 8 | Изучение механизмов определения свежести сообщения . 4 безопасные схемы построения хэш-функций. ПЗ схемы построения электронной цифровой подписи. Процесс генерации ЭЦП. Схема защиты целостности данных. Определение и примеры применения хэш-функции. Асимметричные методы защиты целостности данных: электронная цифровая подпись. Определение и свойства хэш-функции. Электронная цифровая подпись и её свойства. |
| **Дидактическая единица: Аутентификация и идентификация** | | | | |
| 7. Идентификация и аутентификация | 0 | 2 | 1, 10, 12, 13, 6, 8 | Изучение способов аутентификации личности. Коды аутентификации сообщений (MAC). Алгоритм электронной цифровой подписи Эль-Гамаля. Взаимная аутентификация. Аутентификация с помощью пароля. Аутентификация с привлечением доверенного посредника. |
| **Дидактическая единица: Биометрия** | | | | |

| | | | | |
|---|---|---|---|---|
| 8. Введение в биометрию | 0 | 2 | 1, 12, 6, 8 | Изучение основ теории биометрия. Физиологические биометрические параметры, поведенческие биометрические параметры (перечислить не менее 4 шт.). Схема биометрической идентификации, биометрической верификации. Сопоставление биометрических образцов. Схема сопоставления биометрических образцов. 5 свойств биометрических параметров. |

Таблица 3.2

| Темы лабораторных работ | Активные формы, час. | Часы | Ссылки на результаты обучения | Учебная деятельность |
|---|---|---|---|---|
| **Семестр: 3** | | | | |
| **Дидактическая единица: Шифрование с 1 ключом** | | | | |
| 1. Абсолютно стойкий шифр. Применение режима однократного гаммирования. Моделирование работы n-разрядного скремблера | 0 | 5 | 1, 2, 4, 6 | Освоение на практике применение режима однократного гаммирования. Исследование побитного непрерывного шифрования данных. Ознакомление с шифрованием информации при помощи скремблера. |
| 2. Блочные составные шифры и анализ методики многократного использования ключа и материала исходного блока информации (Сеть Фейстеля) | 0 | 5 | 1, 2, 4, 6 | Ознакомление с блочными составными шифрами, освоить криптографические преобразования подстановки и перестановки. Изучение и реализация шифрование информации при помощи сети Фейстеля. |
| 3. Анализ методики многократного использования ключа и материала исходного блока информации (алгоритм DES и российский стандарт шифрования ГОСТ 28147-89) | 0 | 5 | 1, 4, 6 | Изучение алгоритмов симметричного шифрования информации DES и ГОСТ 28147 89. Ознакомление с критериями оценки свойств лавинного эффекта. |
| 4. Режимы работы блочных шифров.Схемы кратного шифрования | 0 | 5 | 1, 4, 6 | Изучение и реализация режимов работы блочных шифров и схемы кратного шифрования для симметричных алгоритмов шифрования DES и ГОСТ 28147 89. |
| **Дидактическая единица: Шифрование с 2 ключами** | | | | |

| | | | | |
|---|---|---|---|---|
| 5. Криптоалгоритмы с открытыми ключами. Генерация простого большого числа.Построение первообразного корня по модулю n. Обмен ключами по схеме Диффи-Хеллмана | 0 | 6 | 1, 5, 6 | Освоение методов генерации больших простых чисел и методы проверки больших чисел на простоту. Ознакомление с теоремой Эйлера, приобретение навыка строить первообразные корни по модулю n. Изучение схему обмена ключами Диффи-Хеллмана. |
| 6. Комбинированные криптоалгоритмы (RSA и DES/ RSA и ГОСТ) | 0 | 5 | 1, 3, 5, 6 | Изучение принципа работы асимметричных алгоритмов шифрования на примере алгоритма RSA. Освоение методики создания комбинированных алгоритмов шифрования, которые совмещают достоинства методов симметричной и асимметричной криптографии. |
| **Дидактическая единица: Целостность** | | | | |
| 7. Электронная цифровая подпись | 0 | 5 | 1, 5, 6 | Изучение различных алгоритмов однонаправленного хэширования данных, основанных на симметричных блочных алгоритмах шифрования. Ознакомление со схемами цифровой подписи и получение навыка создания и проверки подлинности электронной цифровой подписи. |

## 4. Самостоятельная работа обучающегося

| № | Виды самостоятельной работы | Ссылки на результаты обучения | Часы на выполнение | Часы на консультации |
|---|---|---|---|---|
| **Семестр: 3** | | | | |
| 1 | Подготовка к занятиям | 1, 10, 11, 12, 13, 14, 2, 3, 4, 5, 7, 8, 9 | 30 | 6 |

| | | | | |
|---|---|---|---|---|
| Проработка лекционного материала, подготовка к лабораторным работам: Гультяева Т. А. Программные средства защиты информации [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, Н. Л. Долозов, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234876. - Загл. с экрана. Программные средства защиты информации : методические указания к выполнению лабораторных работ для 5 курса по специальности "Прикладная математика и информатика" / Новосиб. гос. техн. ун-т ; [сост. Н. Л. Долозов]. - Новосибирск, 2005. - 69 с. : ил.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2005/2895.rar Программные средства защиты информации : методические указания к выполнению лабораторных работ для 2 курса ФПМИ образовательной программы 02.04.03 - Математическое обеспечение и администрирование информационных систем, магистерские программы - МАтематическое и программное обеспечение информационных технологий и Математическое обеспечение информационных систем в экономике / Новосиб. гос. техн. ун-т ; [сост.: Н. Л. Долозов, С. А. Курлаев, Т. А. Гультяева]. - Новосибирск, 2017. - 96 с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235031 Курлаев С. А. Программные средства защиты информации [Электронный ресурс] : учебно-методическое пособие / С. А. Курлаев, Т. А. Гультяева, Н. Л. Долозов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2011/lib_21369_1322715779.pdf. - Загл. с экрана. | | | | |
| 2 | Подготовка к аттестации | 1, 10, 11, 12, 13, 14, 2, 3, 7, 8, 9 | 10 | 6 |
| Консультации с преподавателем: Гультяева Т. А. Программные средства защиты информации [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, Н. Л. Долозов, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234876. - Загл. с экрана. Гультяева Т. А. Расчетно-графическая работа по курсу "Программные средства защиты информации" [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_1326688273.doc. - Загл. с экрана. Программные средства защиты информации : методические указания к выполнению лабораторных работ для 5 курса по специальности "Прикладная математика и информатика" / Новосиб. гос. техн. ун-т ; [сост. Н. Л. Долозов]. - Новосибирск, 2005. - 69 с. : ил.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2005/2895.rar Программные средства защиты информации : методические указания к выполнению лабораторных работ для 2 курса ФПМИ образовательной программы 02.04.03 - Математическое обеспечение и администрирование информационных систем, магистерские программы - МАтематическое и программное обеспечение информационных технологий и Математическое обеспечение информационных систем в экономике / Новосиб. гос. техн. ун-т ; [сост.: Н. Л. Долозов, С. А. Курлаев, Т. А. Гультяева]. - Новосибирск, 2017. - 96 с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235031 Курлаев С. А. Программные средства защиты информации [Электронный ресурс] : учебно-методическое пособие / С. А. Курлаев, Т. А. Гультяева, Н. Л. Долозов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2011/lib_21369_1322715779.pdf. - Загл. с экрана. | | | | |

## 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 |

## 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: 3** | | |
| *Лабораторная:* | 30 | 60 |
| Контролирующие материалы (список вопросов) приводятся в "Программные средства защиты информации : методические указания к выполнению лабораторных работ для 2 курса ФПМИ образовательной программы 02.04.03 - Математическое обеспечение и администрирование информационных систем, магистерские программы - МАтематическое и программное обеспечение информационных технологий и Математическое обеспечение информационных систем в экономике / Новосиб. гос. техн. ун-т ; [сост.: Н. Л. Долозов, С. А. Курлаев, Т. А. Гультяева]. - Новосибирск, 2017. - 96 с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235031" | | |
| *Экзамен:* | 20 | 40 |
| Контролирующие материалы (список вопросов) приводятся в "Гультяева Т. А. Программные средства защиты информации [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, Н. Л. Долозов, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234876. - 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 | |
|---|---|---|---|
| | | | Экзамен |
| **ОПК.10** | у7. Уметь определять комплекс превентивных мер по защите конфиденциальных данных | | + |
| **ОПК.11** | у1. Уметь формулировать на основе категорий информационной безопасности требования к разрабатываемым средствам защиты информации | | + |
| **ОПК.4** | з1. Знать встроенные средства защиты информации | | + |
| | з5. Знать основные методики создания политики безопасности предприятия с учетом основных рисков информационных атак | | + |
| **ПК.1** | у1. Уметь реализовывать алгоритмы шифрования | | + |

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

## 7. Литература

*Основная литература*

**1.** Нортроп Т. Основы разработки приложений на платформе Microsoft .NET Framework : экзамен-536 MCTS / Тони Нортроп, Шон Уилдермьюс, Билл Райан ; [пер. с англ. А. Е. Соловченко]. - М., 2007. - 842 с. : ил. + 1 CD-ROM.

**2.** Грибунин В. Г. Комплексная система защиты информации на предприятии : [учебное пособие для вузов по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информации" направления подготовки "Информационная безопасность"] / В. Г. Грибунин, В. В. Чудовский. - М., 2009. - 411, [1] с. : ил., табл.

**3.** Васильев, В.И. Интеллектуальные системы защиты информации. [Электронный ресурс] — Электрон. дан. — М. : Машиностроение, 2013. — 172 с. — Режим доступа: http://e.lanbook.com/book/5792 — Загл. с экрана.

**4.** Долозов Н. Л. Программные средства защиты информации : конспект лекций для 2 курса ФПМИ по направлению "Математическое обеспечение и администрирование информационных систем" (02.04.03), магистерская программа, "Математическое и программное обеспечение информационных технологий" / Н. Л. Долозов, Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2015. - 60, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000222753

*Дополнительная литература*

**1.** Галатенко В. А. Основы информационной безопасности : курс лекций : учебное пособие для студентов вузов, обучающихся по специальностям в области информационных технологий / В. А. Галатенко ; под ред. В. Б. Бетелина. - М., 2006. - 205 с. : ил.

**2.** Галатенко В. А. Стандарты информационной безопасности : курс лекций : учебное пособие для студентов вузов, обучающихся по специальностям в области информационных технологий / В. А. Галатенко ; под ред. В. Б. Бетелина. - М., 2006. - 262, [1] с. : табл.

**3.** Столлингс В. Основы защиты сетей. Приложения и стандарты / Вильямс Столлингс ; [пер. с англ. и ред. А. Г. Сивака]. - М. ;, 2002. - 429 с. : ил.

**4.** Галицкий А. В. Защита информации в сети - анализ технологий и синтез решений / Галицкий, А. В. Рябко С. Д., Шаньгин В. Ф. - М., 2004. - 613 с. : ил.

**5.** Мао В. Современная криптография : теория и практика / Венбо Мао ; [пер. с англ. и ред. Д. А. Клюшина]. - М. [и др.], 2005. - 763 с. : ил., табл.

**6.** Зензин О. С. Стандарт криптографической защиты - AES. Конечные поля. - М., 2002. - 174 с. : ил.

**7.** Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : курс лекций : учебное пособие для вузов по специальности 510200 "Прикладная математика и информатика" / О. Р. Лапонина ; под ред. В. А. Сухомлина. - М., 2005. - 604, [1] с. : ил., табл.

**8.** Столлингс В. Криптография и защита сетей. Принципы и практика : пер. с англ. / Вильямс Столлингс. - М., 2001. - 669 с. : ил.

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

**10.** Баричев С. Г. Основы современной криптографии : учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - М., 2002. - 175 с. : ил.

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

**12.** Фергюсон Нильс. Практическая криптография : [пер. с англ.] / Нильс Фергюсон, Брюс Шнайер. - М. : Диалектика : Вильямс, 2005. - 421 с.

**13.** Криптография. Скоростные шифры / А. А. Молдовян, Н. А. Молдовян, Н. Д. Гуц, Б. В. Изотов. – СПб. : БХВ-Петербург, 2002. – 493 с.

**14.** Вельшенбах М. Криптография на Си и С++ в действии : [учеб. пособие] / М. Вельшенбах. – М. : Триумф, 2004. – 461 с. : ил.; 24 см + компакт-диск. - (Практика программирования).

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

*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.** Программные средства защиты информации : методические указания к выполнению лабораторных работ для 5 курса по специальности "Прикладная математика и информатика" / Новосиб. гос. техн. ун-т ; [сост. Н. Л. Долозов]. - Новосибирск, 2005. - 69 с. : ил.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2005/2895.rar

**2.** Курлаев С. А. Программные средства защиты информации [Электронный ресурс] : учебно-методическое пособие / С. А. Курлаев, Т. А. Гультяева, Н. Л. Долозов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2011/lib_21369_1322715779.pdf. - Загл. с экрана.

**3.** Гультяева Т. А. Расчетно-графическая работа по курсу "Программные средства защиты информации" [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_1326688273.doc. - Загл. с экрана.

**4.** Гультяева Т. А. Программные средства защиты информации [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, Н. Л. Долозов, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234876. - Загл. с экрана.

**5.** Программные средства защиты информации : методические указания к выполнению лабораторных работ для 2 курса ФПМИ образовательной программы 02.04.03 - Математическое обеспечение и администрирование информационных систем, магистерские программы - МАтематическое и программное обеспечение информационных технологий и Математическое обеспечение информационных систем в экономике / Новосиб. гос. техн. ун-т ; [сост.: Н. Л. Долозов, С. А. Курлаев, Т. А. Гультяева]. - Новосибирск, 2017. - 96 с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235031

### *8.2 Специализированное программное обеспечение*

**1** Microsoft Office

**2** Visual Studio

**3** MathType

## 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

**Программные средства защиты информации**

Образовательная программа: 02.04.03 Математическое обеспечение и администрирование информационных систем, магистерская программа: Математическое и программное обеспечение информационных технологий

Новосибирск 2015

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

Обобщенная структура фонда оценочных средств по дисциплине Программные средства защиты информации 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.10 владение навыками использования основных моделей информационных технологий и способов их применения для решения задач в предметных областях | у7. Уметь определять комплекс превентивных мер по защите конфиденциальных данных | Ассиметричное шифрование Идентификация и аутентификация Контроль целостности Нарушения, механизмы и службы защиты Симметричное шифрование | | Экзамен: вопросы 55-84<br>Экзамен: задача 12<br>Экзамен: вопросы 85-95<br>Экзамен: вопросы 96-106<br>Экзамен: задача 12<br>Экзамен: вопросы 16-23<br>Экзамен: вопросы 24-54<br>Экзамен: задачи 1, 11 |
| ОПК.11 владение навыками выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования | у1. Уметь формулировать на основе категорий информационной безопасности требования к разрабатываемым средствам защиты информации | Ассиметричное шифрование Введение в биометрию Введение в теорию чисел Идентификация и аутентификация Контроль целостности Нарушения, механизмы и службы защиты Основные понятия криптологии | | Экзамен: вопросы 55-84<br>Экзамен: задача 12<br>Экзамен: вопросы 85-95<br>Экзамен: вопросы 16-23<br>Экзамен: вопросы 107-115<br>Экзамен: задачи 2-10<br>Экзамен: вопросы 1-15<br>Экзамен: задачи 2-10 |
| ОПК.4 владение теоретическими основами информатики как науки; знание проблем современной информатики, ее категории и связи с другими научными дисциплинами, понимание основных этапов и тенденции развития программирования, математического обеспечения и информационных, технологий | з1. Знать встроенные средства защиты информации | Абсолютно стойкий шифр. Применение режима однократного гаммирования. Моделирование работы n-разрядного скремблера Анализ методики многократного использования ключа и материала исходного блока информации (алгоритм DES и российский стандарт шифрования ГОСТ 28147-89) Ассиметричное шифрование Блочные составные шифры и анализ методики многократного использования ключа и материала исходного блока информации (Сеть Фейстеля) Введение в биометрию Идентификация и аутентификация Контроль целостности Нарушения, механизмы и службы защиты Основные понятия криптологии Режимы работы блочных шифров.Схемы кратного шифрования Симметричное шифрование Электронная цифровая | | Экзамен: вопросы 85-95<br>Экзамен: вопросы 16-23<br>Экзамен: вопросы 96-106<br>Экзамен: задача 12<br>Экзамен: вопросы 24-54<br>Экзамен: задачи 1, 11<br>Экзамен: вопросы 1-15<br>Экзамен: вопросы 107-115 |

| | | | | |
|---|---|---|---|---|
| | | подпись | | |
| ОПК.4 | з5. Знать основные методики создания политики безопасности предприятия с учетом основных рисков информационных атак | Ассиметричное шифрование Введение в биометрию Идентификация и аутентификация Контроль целостности Нарушения, механизмы и службы защиты Симметричное шифрование | | Экзамен: вопросы 55-84<br>Экзамен: задача 12<br><br>Экзамен: вопросы 16-23<br><br>Экзамен: вопросы 85-95<br><br>Экзамен: вопросы 24-54<br>Экзамен: задачи 1, 11 |
| ПК.1/НИ владение навыками применения математических основ информатики при разработке и исследовании нового программного обеспечения | у1. Уметь реализовывать алгоритмы шифрования | Абсолютно стойкий шифр. Применение режима однократного гаммирования. Моделирование работы n-разрядного скремблера Анализ методики многократного использования ключа и материала исходного блока информации (алгоритм DES и российский стандарт шифрования ГОСТ 28147-89) Ассиметричное шифрование Блочные составные шифры и анализ методики многократного использования ключа и материала исходного блока информации (Сеть Фейстеля) Введение в биометрию Введение в теорию чисел Идентификация и аутентификация Комбинированные криптоалгоритмы (RSA и DES/ RSA и ГОСТ) Криптоалгоритмы с открытыми ключами. Генерация простого большого числа.Построение первообразного корня по модулю n. Обмен ключами по схеме Диффи-Хеллмана Режимы работы блочных шифров.Схемы кратного шифрования Симметричное шифрование Электронная цифровая подпись | | Экзамен: вопросы 85-95<br><br>Экзамен: вопросы 24-54<br>Экзамен: задачи 1, 11<br><br>Экзамен: вопросы 107-115<br><br>Экзамен: задачи 2-10 |

**2. Методика оценки этапов формирования компетенций в рамках дисциплины.**

Промежуточная аттестация по дисциплине проводится в 3 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОПК.10, ОПК.11, ОПК.4, ПК.1/НИ.

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

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.10, ОПК.11, ОПК.4, ПК.1/НИ, 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 «Программные средства защиты информации», 3 семестр

## 1. Методика оценки

Экзамен проводится в письменной форме, по билетам . Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов (п. 4) 1-55, второй вопрос из диапазона вопросов1-55, третий: 56-77, четвертый: 78-115, пятый-восьмой: *типовые задачи 1-13* . 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 «Программные средства защиты информации»

---

1. Что такое защита информации, информационная безопасность, доступность, целостность, конфиденциальность?
2. 4 вида нарушений защиты (атак): привести подробную характеристику. Пассивные и активные атаки.
3. Что такое простое число, взаимно простые числа? Как можно определить, является ли число простым?
4. Аутентификация с привлечением доверенного посредника. Приведите схему, пояснения.
5. Построить LFSR-генератор, заданный многочленом $g(x) = x^5 + x^2 + 1$ и начальным состоянием $11010_2$, и получить последовательность, содержащую 12 бит.
6. Найти наибольший общий делитель чисел 4307 и 5183.
7. Алгоритмом Евклида найти в поле Галуа полином $b(x)$ такой, что $a(x) \cdot b(x) \equiv 1 \pmod{m(x)}$, если $a(x) = x^5 + x^4 + x + 1$, $m(x) = x^8 + x^6 + x^4 + x^2 + x$.
8. Найти ключи абонента А и абонента В в алгоритме Диффи-Хеллмана при $n = 31$, $x = 12$, $y = 19$. $g$ – выбрать одно из возможных.

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 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 3*4 *баллов.*
- Ответ на экзаменационный билет 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 «**Программные средства защиты информации**»**

*Полный перечень вопросов к экзамену*

1. Что такое защита информации, информационная безопасность?
2. Что такое доступность, целостность, конфиденциальность?
3. 3 аспекта защиты информации.
4. Что такое идентификация, аутентификация?
5. Что представляет собой сервис безопасности «контроль целостности»?
6. Что представляют собой сервисы безопасности «анализ защищённости» и «обеспечение отказоустойчивости»?
7. Что представляет собой сервис безопасности «обеспечение обслуживаемости»?
8. Что представляет собой сервис безопасности «туннелирование»?
9. Что представляет собой сервис безопасности «управление доступом»? В чём заключается суть ролевого управления доступом?
10. Что представляют собой такие сервисы безопасности, как «протоколирование» и «аудит»? Какие задачи решают?
11. Что представляет собой сервис безопасности «экранирование»? Привести подробную схему.

12. Какие атаки называются активными? 4 группы активных атак.
13. Модель защиты сети. Какие задачи нужно решить при разработке конкретного средства защиты?
14. Характеристики, на основе которых строится классификация криптографических систем.
15. 4 вида нарушений защиты (атак): привести подробную характеристику. Пассивные и активные атаки.
16. Что такое криптология, криптография, открытый текст, шифрование, ключ?
17. Что такое криптоанализ? Типы криптоанализа.
18. 2 критерия защищённости схемы шифрования.
19. Что такое защита информации, информационная безопасность, доступность, целостность, конфиденциальность?
20. Что такое шифрование?
21. Что такое абсолютно стойкий шифр?
22. Необходимые и достаточные условия абсолютной стойкости шифра.
23. Что такое лавинный эффект, диффузия и конфузия?
24. Приведите схему симметричной криптосистемы.
25. Какими свойствами должна обладать последовательность, генерируемая скремблером?
26. Что такое примитивный многочлен степени n? Что такое неприводимый многочлен степени n?
27. Преимущества и недостатки использования однократного гаммирования.
28. Преимущества и недостатки использования скремблера.
29. Алгоритм шифрования AES: преобразования сдвига строк (ShiftRows) и добавление раундового ключа (AddRoundKey).
30. В чём заключаются достоинства и недостатки симметричных криптоалгоритмов?
31. Что такое примитивный многочлен степени n? Что такое неприводимый многочлен степени n?
32. Что такое скремблер, сдвиговый регистр с обратной связью (LFSR)? Приведите схему работы LFSR.
33. Сравните алгоритмы DES и ГОСТ 28147-89. Достоинства и недостатки каждого алгоритма.
34. Распределение ключей при симметричном шифровании.
35. Сценарий централизованного распределения ключей при симметричном шифровании.
36. Сценарий децентрализованного распределения ключей при симметричном шифровании.
37. Сеть Фейстеля. В чём заключаются процессы шифрования и дешифрования?
38. Алгоритм шифрования DES. Общая схема.
39. Алгоритм шифрования DES. В чём заключается функция шифрования f?
40. Алгоритм шифрования DES. Алгоритм получения раундовых ключей.
41. Режим электронной шифровальной книги (ECB). Привести уравнения и нарисовать блок-схему процесса шифрования.
42. Режим сцепление шифрованных блоков (CBC). Привести уравнения и нарисовать блок-схему процесса шифрования.

43. Режим обратная связь по шифротексту (CFB). Привести уравнения и нарисовать блок-схему процесса шифрования.
44. Режим обратная связь по выходу (OFB). Привести уравнения и нарисовать блок-схему процесса шифрования.
45. Схема двойного шифрования. В чём заключается метод двусторонней атаки?
46. 2 схемы тройного шифрования. Привести уравнения и нарисовать блок-схему процесса шифрования. Какая схема лучше и почему?
47. Алгоритм шифрования ГОСТ 28147-89. Общая схема. Описание функции шифрования f.
48. Алгоритм шифрования AES: общий алгоритм.
49. Алгоритм шифрования AES: преобразование замена байт (SubBytes).
50. Алгоритм шифрования AES: преобразование замешивания столбцов (MixColumns).
51. Алгоритм шифрования AES: алгоритм выработки ключей (Key Schedule).
52. Сценарий централизованного распределения ключей при симметричном шифровании.
53. Режим обратная связь по шифротексту (CFB). Привести уравнения и нарисовать блок-схему процесса шифрования.
54. Режим обратная связь по выходу (OFB). Привести уравнения и нарисовать блок-схему процесса шифрования.
55. Что такое простое число, взаимно простые числа? Как можно определить, является ли число простым?
56. Определение и свойства функции Эйлера.
57. Малая теорема Ферма.
58. Теорема Эйлера.
59. Как сгенерировать большое простое число?
60. В чём заключается безопасность обмена ключа по схеме Диффи-Хеллмана?
61. Почему криптосистемы с открытым ключом на практике используются только для шифрования ключа, но не открытого текста?
62. В чём заключаются достоинства и недостатки асимметричных криптоалгоритмов?
63. Приведите схему асимметричной криптосистемы.
64. Приведите схему асимметричной криптосистемы.
65. В чём заключаются достоинства и недостатки асимметричных криптоалгоритмов?
66. Что такое простое число, взаимно простые числа? Как можно определить, является ли число простым?
67. Что означает решить сравнение? Какими методами можно решать сравнение? Общий вид решения сравнения первой степени.
68. Определение и свойства первообразных корней и числа, принадлежащего показателю n.
69. В чём заключается алгоритм Евклида?
70. В чём заключается расширенный алгоритм Евклида?
71. Решение сравнения первой степени способом Эйлера.
72. Алгоритм шифрования RSA.
73. Схема обмена ключами Диффи-Хеллмана.
74. В чём заключается алгоритм Евклида?
75. В чём заключается расширенный алгоритм Евклида?
76. Решение сравнения первой степени с помощью алгоритма Евклида.

77. Решение сравнения первой степени с помощью расширенного алгоритма Евклида.
78. Алгоритм Рабина-Миллера.
79. Распределение открытых ключей в асимметричной криптосистеме: метод «публичное объявление».
80. Распределение открытых ключей в асимметричной криптосистеме: метод «публично доступный каталог».
81. Распределение открытых ключей в асимметричной криптосистеме: метод «авторитетный источник ключей».
82. Распределение открытых ключей в асимметричной криптосистеме: метод «сертификаты открытых ключей». Какие требования существуют для этого метода?
83. Распределение секретных ключей в асимметричной криптосистеме: метод «распределение ключей с обеспечением конфиденциальности и аутентификации».
84. Распределение секретных ключей в асимметричной криптосистеме: метод «простое распределение ключей» (схема Меркла). Приведите пример того, как этот протокол может быть скомпрометирован.
85. 3 способа аутентификации личности.
86. Коды аутентификации сообщений (MAC) с использованием функции хэширования с ключом.
87. Коды аутентификации сообщений (MAC) с использованием алгоритмов блочного шифрования.
88. Алгоритм электронной цифровой подписи RSA.
89. Алгоритм электронной цифровой подписи Эль-Гамаля.
90. Что такое идентификация, аутентификация? Подробное описание 3 видов аутентификации.
91. Взаимная аутентификация. Приведите схему.
92. Аутентификация с помощью пароля: простейший протокол. Приведите схему. Укажите, какие существуют проблемы у данного подхода.
93. Аутентификация с помощью пароля: протокол Нидхема. Приведите схему. Укажите, какие существуют проблемы у данного подхода.
94. Аутентификация с помощью пароля: схема с одноразовыми паролями. Приведите схему. Укажите, какие существуют проблемы у данного подхода.
95. Аутентификация с привлечением доверенного посредника. Приведите схему, пояснения.
96. Механизмы определения свежести сообщения и существования пользователя: стратегии оклик-отзыв – 3 варианта (схемы, пояснения); стандартные варианты этих стратегий (схемы, пояснения).
97. Механизмы определения свежести сообщения и существования пользователя: метка времени – 3 варианта (схемы, пояснения); стандартные варианты этих стратегий (схемы, пояснения).
98. 4 безопасные схемы построения хэш-функций. Привести схемы, пояснения.
99. 3 схемы построения электронной цифровой подписи. Процесс генерации ЭЦП.
100. Приведите схему защиты целостности данных.
101. Приведите определение и примеры применения хэш-функции.
102. Асимметричные методы защиты целостности данных: электронная цифровая подпись. Приведите схему, примеры алгоритмов.
103. Определение и свойства хэш-функции.

104. Электронная цифровая подпись и её свойства.
105. Приведите схему защиты целостности данных.
106. Приведите определение и примеры применения хэш-функции.
107. Что такое биометрия?
108. Физиологические биометрические параметры (перечислить не менее 5 шт.).
109. Поведенческие биометрические параметры (перечислить не менее 4 шт.).
110. (2) Приведите схему биометрической идентификации.
111. Приведите схему биометрической верификации.
112. Сопоставление биометрических образцов. Что такое биометрический шаблон? Приведите схему сопоставления биометрических образцов.
113. Что такое верификация и идентификация в биометрии?
114. 5 свойств биометрических параметров.
115. Какие задачи можно решать с помощью биометрии?

*Перечень типовых задач к экзамену*

1. Построить LFSR-генератор, заданный многочленом $g(x) = x^5 + x^2 + 1$ и начальным состоянием $11010_2$, и получить последовательность, содержащую 12 бит.
2. Найти функцию Эйлера для числа 4725.
3. Найти наибольший общий делитель чисел 4307 и 5183.
4. Умножить полином $a(x) = x^3 + x^2 + x$ на полином $b(x) = x^5 + x^4 + x^2 + x + 1$ в поле Галуа по модулю полинома $m(x) = x^5 + x^2 + 1$.
5. Найти наибольший первообразный корень для числа 50.
6. Решить сравнение 113 $x \equiv 58 \pmod{259}$ способом Эйлера.
7. Найти алгоритмом Евклида элемент $d$ такой, что $e \cdot d \equiv 1 \pmod{n}$, если $e = 88$, $n = 107$.
8. Найти все первообразные корни для числа 6.
9. Решить сравнение 195 $x \equiv 141 \pmod{342}$ алгоритмом Евклида.
10. Алгоритмом Евклида найти в поле Галуа полином $b(x)$ такой, что $a(x) \cdot b(x) \equiv 1 \pmod{m(x)}$, если $a(x) = x^5 + x^4 + x + 1$, $m(x) = x^8 + x^6 + x^4 + x^2 + x$.
11. Найти ключи абонента А и абонента В в алгоритме Диффи-Хеллмана при $n = 31$, $x = 12$, $y = 19$. $g$ – выбрать одно из возможных.
12. Найти открытый и закрытый ключи, зашифровать сообщение $M = 7$ с помощью алгоритма RSA. $p = 3$, $q = 11$, $e$ – выбрать одно из возможных, $d$ – найти одним из методов (не подбором). Привести подробное решение.
13. Найти открытый и закрытый ключи и сгенерировать электронную цифровую подпись по алгоритму Эль-Гамаля для сообщения $M = 14$, если $p = 7$, $g = 6$, $x = 5$.