Министерство образования и науки РФ

Государственное образовательное учреждение высшего профессионального образования

**«Санкт-Петербургский государственный электротехнический университет “ЛЭТИ” им. В.И. Ульянова (Ленина)» (СПбГЭТУ)**

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Теоретико-числовые методы в криптографии»*

Для подготовки дипломированных специалистов по специальности 090102.65

*«Компьютерная безопасность»*

Санкт-Петербург

2011

Санкт-Петербургский государственный электротехнический

университет “ЛЭТИ”

"УТВЕРЖДАЮ"

проректор по учебной работе

Лысенко Н.В.

"\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_2011 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Теоретико-числовые методы в криптографии»*

Для подготовки дипломированных специалистов по специальности 090102.65

*«Компьютерная безопасность»*

Уч.план № 339

Факультет компьютерных технологий и информатики

Кафедра автоматизированных систем обработки информации и управления

Курс – 4

Семестр – 8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 34 ч. |  | Экзамен | 8 семестр |
|  |  |  |  |  |
| Практические занятия | 17 ч. |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
| Аудиторные занятия | 51 ч. |
| Самостоятельные занятия | 40 ч. |
| Всего часов | 91 ч. |

2011 г.

Рабочая программа обсуждена на заседании кафедры Автоматизированных систем обработки информации и управления «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2011 г., протокол № \_\_\_\_.

Рабочая программа составлена в соответствии с государственным образовательным стандартом для дипломированных специалистов по специальности

090102.65 — «Компьютерная безопасность»

Дисциплина «Теоретико-числовые методы в криптографии» преподается на основе изученных ранее дисциплин:

* Алгебра и геометрия;
* Математический анализ;
* Дискретная математика
* Вычислительная математика;
* Теория вероятностей и математическая статистика;
* Теоретические основы компьютерной безопасности;
* Теория информационных процессов и систем

и обеспечивает изучение следующих дисциплин:

* Криптографические протоколы;
* Криптографические методы защиты информации.

Рабочая программа одобрена методической комиссией факультета компьютерных технологий и информатики «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2011 г.

Аннотация дисциплины

В дисциплине излагаются основные понятия и методы теории чисел с ее приложениями в современной криптографии, теория сложности алгоритмы (вычисления), комбинаторики, теория чисел и приложение этих методов в криптографии и криптоанализе. Основное внимание уделено изучению задач и алгоритмов, положенных в основу современных криптографических систем и протоколов. Приведены алгоритмы решения этих задач и оценка сложности этих задач на вычислителе. Дисциплина относится к числу прикладных математических дисциплин в силу отбора изучаемого материала и его важности для подготовки специалиста.

**Цели и задачи дисциплины**

Дисциплина обеспечивает приобретение знаний по математическим основам криптографической защиты информации. Целью преподавания дисциплины является изложение базовых принципов построения и математического обоснования криптографических систем.

Задачи изложить:

* алгебраические, аналитические и вероятностные подходы к построению и анализу криптосистем;
* математические основы криптографии;
* математические методы, используемые в криптоанализе.

**Требования к уровню освоения дисциплины**

В результате изучения дисциплины студенты должны

иметь представление:

* об основных задачах и понятиях криптографии;
* о видах информации, подлежащей шифрованию:
* о классификации шифров:
* о методах криптографического синтеза и анализа;
* о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи;
* о методах криптозащиты компьютерных систем и сетей;
* об основных подходах к изучению криптосистем;
* об основных алгоритмических проблемах криптографии и способах их решения;
* о специальных математических структурах, применяемых в криптографии;

знать:

* основные принципы кодирования и декодирования при передаче сообщений;
* принципы построения различных кодов;
* применение теории вероятности в криптографии и криптоанализе;

уметь:

* формализовать поставленную задачу;
* выполнить постановку задач криптоанализа и указать подходы к их решению;
* использовать основные математические методы, применяемые в синтезе и анализе типовых криптографических алгоритмов;

иметь навыки:

* владения криптографической терминологией;
* навыками использования основных типов кодов.

Содержание рабочей программы

**Тема 1. Теория информации — математическая основа для синтеза и анализа симметричных (одноключевых) шифров**

Скорость языка. Избыточность языка. Ненадёжность ключа. Модель случайного шифра Шеннона. Количественная оценка стойкости шифра — расстояние единственности шифра, формула для вычисления расстояния единственности. Совершенно секретные шифры. Теорема о совершенной секретности.

**Тема 2. Теория сложности алгоритмов как математическая основа для синтеза и анализа двуключевых криптографических систем (систем с открытыми ключами)**

Определение, основные понятия. Временная и пространственная сложность. Современная классификация сложности решения задач (выполнение алгоритмов). NP-полные задачи, положенные в основу построение систем с открытыми ключами. Однонаправленные функцив. Однонаправленные функции с лазейкой. Сложность основных целочисленных алгоритмов в конечных полях, кольцев вычетов и кольце целых чисел.

**Тема 3. Основы теории чисел**

Простые числа, псевдопростые числа. Асимптотический закон распределения простых чисел (теорема Чебышева). Методы построения больших простых чисел. Тесты на простоту: вероятностный и детерминированный.

**Тема 4. Сложность основных целочисленных алгоритмов в конечных полях, кольцев вычетов и кольце целых чисел**

Конечные поля: простые и расширенные конечные поля. Кольцо целых чисел. Вычеты, невычеты, кольцо вычетов.

**Темы 5. Задачи разложения составного числа на простые сомножители (система RSA)**

Система вычетов по модулю простого числа, система вычетов по модулю составного числа. Функция Эйлера. Теорема Ферма. Расширенный алгоритм Евклида. Китайская теорема об остатках. Выбор параметров в системе RSA. Вычисление закрытого ключа. Оценка стойкости.

**Тема 6. Задача дискретного логарифмирования в конечном поле**

Методы решения задачи дискретного логарифмирования: методы встречи по-середине, метод Поллард-Силвера, метод Ленстра. Протокол Диффи-Хеллмана. Выбор параметров протокола. Оценка криптостойкости.

**Тема 7. Задача декодирования линейного блокового кода с неизвестной порождающей (проверочной) матрицей**

Линейный блоковый код. Способы задания линейного блокового кода. Основные алгоритмы декодирования линейных блоковых кодов. Корректирующая способность линейных блоковых кодов. Система Мак-Элиса как пример системы для постквантумной криптографии. Выбор параметров системы Мак-Элиса. Коды Гоппа.

**Перечень практических занятий**

|  |  |  |
| --- | --- | --- |
| № | Наименование темы занятия | Номер темы программы |
| 1 | Математическая основа для построения симметричных шифров в теории информации: вычисление расстояния единственности DES и ГОСТ 28147-89 | 1 |
| 2 | Система RSA: вычисление ключей, расширенный алгоритм Евклида и быстрое возведение в степень. | 2,5 |
| 3 | Решение задачи дискретного логарифмирования в конечном поле: протокол Диффе-Хеллмана, ЭЦП ElGamale. | 3,6 |

**Распределение учебных часов по темам, видам занятий**

**и видам самостоятельной работы**

| № темы | Название разделов и тем | **Объем учебных часов** | | | | | | Семестр | Литература по темам |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Лекции | Лабор. занят. | Практ. занят. | Аудит. занят. | Самост. Работа | **Всего** |
| 1 | Теория информации — математическая основа для синтеза и анализа симметричных (одноключевых) шифров | 4 |  | 4 | 8 | 6 | 14 | 8 | Л1, Л3, Д3, Д4 |
|
| 2 | Теория сложности алгоритмов как математическая основа для синтеза и анализа двуключевых криптографических систем (систем с открытыми ключами) | 8 |  | 2 | 10 | 6 | 16 | 8 | Л3, Д2, Д4, Д5 |
|
| 3 | Основы теории чисел | 6 |  | 3 | 9 | 6 | 15 | 8 | Л3, Д1, Д4, Д5 |
|
| 4 | Сложность основных целочисленных алгоритмов в конечных полях, кольцев вычетов и кольце целых чисел | 6 |  |  | 6 | 6 | 12 | 8 | Л4, Д1, Д4, Д5 |
|
| 5 | Задачи разложения составного числа на простые сомножители (система RSA) | 2 |  | 4 | 6 | 6 | 12 | 8 | Л1, Л4,  Д3, Д4 |
| 6 | Задача дискретного логарифмирования в конечном поле | 4 |  | 4 | 8 | 6 | 14 | 8 | Л1, Л2,  Д1, Д2 |
| 7 | Задача декодирования линейного блокового кода с неизвестной порождающей (проверочной) матрицей | 4 |  |  | 4 | 4 | 8 | 8 | Л1, Д3 |
| ИТОГО: | | 34 |  | 17 | 51 | 40 | 91 | 8 |

# Учебно-методическое обеспечение дисциплины

# Основная литература

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название, библиографическое описание | Л | Лр | Пз (С) | Кп | Кр | К-во экз. в библ. (на каф.) | Гриф |
| **Л1** | Дернова Е.С., Молдовян Н.А., Молдовяну П.А. Элементы теоретических основ криптографии. - СПб., Изд. СПбГЭТУ, 2009. – 92 с. | 8 |  | 8 |  |  | У(72) |  |
| **Л2** | Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение/Р. Морелос-Сарагоса ; пер. с англ. В.Б. Афанасьева. - 2005 | 8 |  | 8 |  |  | У(25) |  |
| **Л3** | Вернер М. Основы кодирования/М. Вернер; пер. с нем. Д.К. Зигангирова. - 2004 | 8 |  | 8 |  |  | У(19) |  |
| **Л4** | Шнайер, Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си - М. : ТРИУМФ, 2003 | 8 |  | 8 |  |  | Ф(2) |  |

##### Дополнительная литература

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| **Д1** | Питерсон У. Коды, исправляющие ошибки/У. Питерсон; пер. с англ.Е. Филипповой ; под ред. [и с предисл.] Р.Л. Добрушина. - 1964 | Ф(2) |
| **Д2** | Харкевич А.А. Борьба с помехами/А.А. Харкевич. - 1965 | У(18) |
| **Д3** | Кузьмин И.В. Основы теории информации и кодирования/И.В. Кузьмин. - 1977 | У(9) |
| **Д4** | Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963. | У(6) |
| **Д5** | Дадаев Ю.Г. Теория арифметических кодов/Ю.Г. Дадаев. - 1981 | Ф(1) |

|  |  |
| --- | --- |
| Зав. отделом учебной литературы *(для технических дисциплин)* | Киселева Т.В |

|  |  |
| --- | --- |
| Автор: |  |
| к.т.н., доцент | Шашин А.М. |
|  |  |
| Рецензент |  |
| д.т.н., профессор | Водяхо А.И. |
|  |  |
| Зав. кафедрой автоматизированных систем обработки информации управленияи и управления |  |
| д.т.н., профессор | Советов Б.Я. |
|  |  |
| Декан факультета компьютерных технологий и информатики |  |
| д.т.н., профессор | Куприянов М.С. |
|  |  |
| Программа согласована: |  |
|  |  |
| Председатель методической комиссии факультета *компьютерных*  *технологий и информатики* |  |
| к.т.н., доц. | Михалков В.А. |
|  |  |
| Руководитель методического отдела |  |
| к.т.н., доцент | Марасина Л.А. |
|  |  |