Министерство образования и науки РФ

Государственное образовательное учреждение высшего профессионального образования

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

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Теоретико-числовые методы в криптографии»*

Для подготовки дипломированных специалистов по специальности 090301.65

*«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 090301.65

*«Компьютерная безопасность»*

Уч.план № 836

Факультет компьютерных технологий и информатики

Кафедра автоматизированных систем обработки информации и управления

Курс – 4

Семестр – 7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 54 ч. |  | Экзамен | 7 семестр |
|  |  |  |  |  |
| Практические занятия | 36 ч. |  |  |  |

|  |  |
| --- | --- |
| Аудиторные занятия | 90 ч. |
| Самостоятельные занятия | 80 ч. |
| Всего часов | 170 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

090301.65 — «Компьютерная безопасность»

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

* Алгебра и геометрия;
* Математический анализ;
* Вычислительная математика;
* Теория вероятностей и математическая статистика;
* Основы информационной безопасности;

и обеспечивает изучение следующих дисциплин:

* 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, ознакомление с методами оценки сложности применяемых на практике

кодов и построения эффективных кодов для решения некоторых прикладных задач в области информационной безопасности. 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**

Изучение дисциплины направлено на формирование вклада в следующие компетенции:

*ПК-2* – способность применять математический аппарат, в т.ч. с использованием ВТ, для решения профессиональных задач;

*ПК-9* – способность использовать языки и системы программирования, инструментальные средства для решения различных профессиональны, исследовательских и прикладных задач;

*ПК-12* – способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

*ПК-16* – способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности;

*ПК-18* – способность разрабатывать математические модели безопасности защищаемых компьютерных систем.

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;

иметь навыки:

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

Содержание рабочей программы

**Тема 1. Основные принципы кодирования и декодирования при передаче сообщений**

Блоковое и неблоковое кодирование. Модели каналов связи. Основные принципы декодирования. Объем шара Хэмминга. Способность кода обнаруживать и исправлять ошибки. Границы для минимального расстояния.

**Тема 2. Линейные коды**

Линейные коды. Синдромное декодирование линейных кодов. Вероятностные характеристики декодирования в каналах с независимыми ошибками.

**Тема 3. Циклические коды**

Определение и свойства циклических кодов. Многотактные линейные фильтры. Вычислители остатков. Реализация операции кодирования для циклических кодов. Синдромное декодирование циклических кодов.

**Тема 4. Коды Боуза-Чоудхури-Хоквингхема (БЧХ-Коды)**

Алгебраическое декодирование циклических кодов. Матрица Вандермонда. Коды Боуза-Чоудхури-Хоквингхема. Декодирование БЧХ-кодов.

**Перечень практических занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование темы занятия | Номер темы программы | Трудоемкость |
| 1 | Построение линейных кодов и их декодирование | 2 | 8 |
| 2 | Построение циклических кодов и их декодирование | 3 | 12 |
| 3 | Построение БЧХ-кодов и их декодирование | 4 | 16 |

**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.** | | **Сам.**  **работа** | **Всего** |
| **Всего** | **в т.ч. инт.формы** |
| 1 | Основные принципы кодирования и декодирования при передаче сообщений | 10 |  |  | 10 |  | 12 | 22 | 7 | **Л1, Л3, Д3, Д4** |
| 2 | Линейные коды | 18 |  | 8 | 26 | 8 | 24 | 50 | 7 | **Л3, Д2, Д4, Д5** |
| 3 | Циклические коды | 16 |  | 12 | 28 | 12 | 20 | 48 | 7 | **Л3, Д1, Д4, Д5** |
| 4 | Коды Боуза-Чоудхури-Хоквингхема (БЧХ-Коды) | 10 |  | 16 | 26 | 16 | 24 | 50 | 7 | **Л2, Д1, Д4, Д5** |
| ИТОГО: | | 54 |  | 36 | 90 | 36 | 80 | 170 |  |

**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. | 7 |  |  |  |  | У(72) |  |
| **Л2** | Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение/Р. Морелос-Сарагоса ; пер. с англ. В.Б. Афанасьева. - 2005 | 7 |  | 7 |  |  | У(25) |  |
| **Л3** | Вернер М. Основы кодирования/М. Вернер; пер. с нем. Д.К. Зигангирова. - 2004 | 7 |  | 7 |  |  | У(19) |  |

##### 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) |
| **Л2** | Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963. | У(6) |
| **Л3** | 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. |
|  |  |