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

*«Теоретические основы компьютерной безопасности»*

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

*«Теоретические основы компьютерной безопасности»*

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 – 7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 36 ч. |  | Текущий контроль | 7 семестр |
|  |  |  |  |  |
| Практические занятия | 18 ч. |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
| Аудиторные занятия | 54 ч. |
| Самостоятельные занятия | 52 ч. |
| Всего часов | 106 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 «Теоретические основы компьютерной безопасности» преподается на основе изученных ранее дисциплин:

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

и является фундаментом для изучения следующих дисциплин:

* Криптографические методы защиты информации;
* Технические средства и методы защиты информации;
* Теоретико-числовые методы в криптографии.

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

Аннотация дисциплины

Дисциплина посвящена изучению математической базы защиты информации. Лекционный курс состоит из двух глав, содержащих одиннадцать тем. Рассматривается материал, имеющий приложение в современной криптографии: основные элементы дискретной алгебры и арифметики полей Галуа.

**Цели и задачи дисциплины**

1. Изучение математического аппарата, составляющего основу методов обеспечения компьютерной безопасности.
2. Приобретение навыков использования математических методов для решения задач обеспечения информационной безопасности.

**Требования к уровню освоения дисциплины**

В результате изучения дисциплины студенты должны:

1. Знать математический аппарат, составляющий основу методов обеспечения информационной безопасности.
2. Уметь применять различные математические методы и модели при разработке криптографических систем и протоколов.

Содержание рабочей программы

**Глава 1. Введение в дискретную алгебру.**

* 1. **Группы.** Определение группы. Теорема о единичном и обратном элементе. Подгруппы. Циклические группы и их свойства. Разложение группы на левые и правые смежные классы по подгруппе. Теорема о разложении группы на смежные классы. Теорема о порядке конечной группы.
  2. **Кольца.** Определение кольца. Теорема о коммутативности нуля и ассоциативности обратного элемента в кольце, для любых элементов кольца. Теорема о кольце с единицей. Теорема о множестве единиц кольца.
  3. **Поля.** Определения поля, примеры. Определение расширения поля. Теорема о условии сокращения. Определение области целостности.
  4. **Векторные пространства.** Определение векторного пространства. Линейная комбинация векторов. Линейно зависимые и линейно независимые вектора. Теорема о векторном пространстве и количестве ЛНЗ векторов. Теорема о равенстве количества векторов при порождении ими одного и того же векторного пространства. Теорема о базисе векторного пространства. Теорема о дополнении множества ЛНЗ векторов до базиса. Теорема о подпространстве векторного пространства. Теорема о размерности векторного подпространства. Скалярное произведение векторов. Теорема о множестве векторов, ортогональных к векторному подпространству. Теорема о ортогональном дополнении подпространства.
  5. **Линейная алгебра.** Определение матрицы. Главная диагональ. Квадратная и единичная матрицы. Правила сложения и умножения матриц. Транспонированная матрица. Определитель матрицы. Теорема о определителе матрицы. Минор и алгебраическое дополнение. Пространство столбцов, строк и ранг матрицы. Элементарные операции над строками матрицы. Канонический ступенчатый вид матрицы. Теорема о совпадении пространства строк матриц, полученных с помощью элементарных операций над строками. Теорема о числе линейно независимых столбцов в матрице. Теорема о равенстве ранга матрицы по строкам и по столбцам. Теорема о вычислении определителя произведения матриц. Теорема о размерности ортогонального дополнения подпространства векторного пространства.

**Глава 2. Арифметика полей Галуа.**

2.1 **Кольцо целых чисел.** Делитель. Простые и составные числа. Наименьшее общее кратное и наибольший общий делитель. Теорема о делении с остатком. Алгоритм Евклида. Расширенный алгоритм Евклида.

2.2 **Конечные поля, основанные на кольце целых чисел.** Определение кольца отношений (кольца целых чисел). Теорема о принадлежности колец целых чисел к кольцам. Теорема о принадлежности кольца целых чисел к полям. Китайские теоремы об остатках.

2.3 **Кольца многочленов.** Определение многочлена, неопределенной переменной, нулевого многочлена, приведенного многочлена, степени ненулевого многочлена. Сумма и произведение многочленов. Деление многочленов с остатком, неприводимый и простой многочлены. НОД и НОК двух многочленов. Определение формальной производной. Теорема о делении многочленов с остатков (алгоритм деления для многочленов). Теорема об остатках от деления многочленов. Теорема об однозначном разложении многочлена над некоторым полем. Алгоритм Евклида для многочленов. Теорема о корнях многочлена. Китайские теоремы об остатках для многочленов.

2.4 **Конечные поля, основанные на кольцах многочленов.** Определение кольца многочленов по модулю. Теорема о принадлежности множества многочленов по модулю к кольцам. Теорема о принадлежности кольца многочленов, приведенных по модулю к полям. Поля Галуа. Пример поля Галуа GF(4). Простые многочлены над полем Галуа GF(2). Основные свойства полей Галуа.

2.5 **Примитивные элементы.** Определение примитивного элемента поля GF(q). Теорема о ненулевых элементах GF(q). Теорема о цикличности группы ненулевых элементов поля GF(q). Теорема о примитивном элементе для полей Галуа. Определение примитивного многочлена над полем Галуа

2.6 **Структура конечного поля.** Определение характеристики поля Галуа. Теорема о подполе поля Галуа и характеристика поля. Определение минимального многочлена над полем Галуа. Теорема о минимальном многочлене. Теорема о расширении поля Галуа. Определение поля разложения многочлена. Теорема о числе элементов расширения поля. Теорема о количестве элементов в поле разложения многочлена. Теорема о существовании простого многочлена над каждым конечным полем Галуа.

**Перечень практических занятий**

|  |  |  |
| --- | --- | --- |
| № | Наименование темы занятия | Номер темы программы |
| 1 | Векторные пространства | 4 |
| 2 | Линейная алгебра | 5 |

**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 | Группы | 2 |  |  | 2 | 2 | 4 | 7 | Л1, Л2 |
|
| 2 | Кольца | 2 |  |  | 2 | 2 | 4 | 7 | Л1, Л2 |
|
| 3 | Поля | 4 |  |  | 4 | 4 | 8 | 7 | Л1 |
|
| 4 | Векторные пространства | 6 |  | 8 | 14 | 14 | 28 | 7 | Л1, Д1 |
|
| 5 | Линейная алгебра | 6 |  | 10 | 16 | 14 | 30 | 7 | Л1 |
|
|
| 6 | Кольцо целых чисел | 2 |  |  | 2 | 2 | 4 | 7 | Л1, Л2 |
| 7 | Конечные поля, основанные на кольце целых чисел | 2 |  |  | 2 | 2 | 4 | 7 | Л1, Л2 |
| 8 | Кольца многочленов | 4 |  |  | 4 | 4 | 8 | 7 | Л1, Л2 |
| 9 | Конечные поля, основанные на кольцах многочленов | 4 |  |  | 4 | 4 | 8 | 7 | Л1, Л2 |
| 10 | Примитивные элементы | 2 |  |  | 2 | 2 | 4 | 7 | Л1, Л2 |
| 11 | Структура конечного поля | 2 |  |  | 2 | 2 | 4 | 7 | Л1, Л2 |
| ИТОГО: | | 36 |  | 18 | 54 | 52 | 106 | 7 |

# Учебно-методическое обеспечение дисциплины

# Основная литература

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название, библиографическое описание | Л | Лр | Пз (С) | Кп | Кр | К-во экз. в библ. (на каф.) | Гриф |
| **Л1** | Молдовян Н.А. Алгоритмы аутентификации информации в АСУ на основе структур в конечных векторных пространствах/Н. А. Молдовян // Автоматика и телемеханика. -М.:Наука, 2008,N №12.-С.163-177 | 10 |  | 10 |  |  | Каф. (5) |  |

##### Дополнительная литература

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| **Л1** | Ляпин Е.С. Алгебра и теория чисел. Ч.1: Числа. - 1974 | Ф(1) |
| **Л2** | Группы, кольца, поля : Метод. указания по дисциплине "Геометрия и алгебра"./Санкт-Петербургский государственный электротехнический университет им. В.И. Ульянова (Ленина) "ЛЭТИ" . - 1997 | ЧЗ1(5)  Ф(4) |

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

|  |  |
| --- | --- |
| Авторы: |  |
| 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. |