

**АННОТАЦИЯ**  
дисциплины «Б1.В.ДВ.09.02 ТЕОРЕТИКО-ГРУППОВЫЕ МОДЕЛИ В КОДИРОВАНИИ  
И ЗАЩИТЕ ИНФОРМАЦИИ»

**Объем трудоемкости:** 3 зачетные единицы (108 часа, из них – 68,2 часа контактной работы (32 часа лекций, 32 часа лабораторных занятий, 11 часов КСР, 0,2 часа ИКР); 32,8 часа самостоятельной работы).

**Цель дисциплины:**

Цель освоения дисциплины – знакомство с задачами и методами защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук. Ее значение возрастает в свете ведущейся информационной войны против Российской Федерации.

**Задачи дисциплины:**

Задачи освоения дисциплины «Теоретико-групповые модели в кодировании и защите информации»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета и получение сведений:

о компьютерной реализации информационных объектов;

связи компьютерной алгебры и численного анализа;

об основных задачах и понятиях криптографии;

об этапах развития 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.

**Место дисциплины в структуре ООП ВО**

Дисциплина «Теоретико-групповые модели в кодировании и защите информации» относится к профессиональному циклу (Б1) к курсам естественно-научного содержания (Б1.В.ДВ.09.02).

Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов.

**Требования к уровню освоения дисциплины**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

| № п.п. | Индекс компетенции | Содержание компетенции (или её части)                                                                                                                  | В результате изучения учебной дисциплины обучающиеся должны              |                                                                            |                                                                                                          |
|--------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
|        |                    |                                                                                                                                                        | знать                                                                    | уметь                                                                      | владеть                                                                                                  |
| 1.     | ОПК-2              | Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- | О компьютерной реализации информационных объектов.<br>Связи компьютерной | Определять структуры данных в компьютерной алгебре.<br>использовать техни- | навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа про- |

| № п.п. | Индекс компетенции | Содержание компетенции (или её части)                                                                                                                                                                                                                                    | В результате изучения учебной дисциплины обучающиеся должны                                                                                     |                                                                                                                              |                                                                                                                                                       |
|--------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                    |                                                                                                                                                                                                                                                                          | знать                                                                                                                                           | уметь                                                                                                                        | владеть                                                                                                                                               |
| 2.     | ОПК-4              | коммуникационных технологий и с учетом основных требований информационной безопасности<br>Способность находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем | алгебры и численного анализа. Элементы теории сложности алгоритмов. об основных задачах и понятиях криптографии об этапах развития криптографии | ку символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифр-систем. | стейших шифров: навыками математического моделирования в криптографии; современной научнотехнической литературой в области криптографической защиты.. |
| 3      | ПК-4               | способностью публично представлять собственные и известные научные результаты                                                                                                                                                                                            |                                                                                                                                                 |                                                                                                                              |                                                                                                                                                       |

#### Основные разделы дисциплины:

| № | Наименование разделов                                                           | Количество часов |                   |    |    |                      |
|---|---------------------------------------------------------------------------------|------------------|-------------------|----|----|----------------------|
|   |                                                                                 | Всего            | Аудиторная работа |    |    | Внеаудиторная работа |
|   |                                                                                 |                  | Л                 | ПЗ | ЛР | СРС                  |
| 1 | 2                                                                               | 3                | 4                 | 5  | 6  | 7                    |
| 1 | Теоретико-числовые конструкции в теории защиты информации и теории кодов        | 26               | 8                 |    | 8  | 10                   |
| 2 | Основы алгебраической теории кодов                                              | 22               | 8                 |    | 8  | 6                    |
| 3 | Теоретико-числовые модели защищенных информационных систем                      | 24               | 8                 |    | 8  | 8                    |
| 4 | Поточные шифры. Синхронизированные и самосинхронизирующиеся. Надежность шифров. | 18,8             | 8                 |    | 8  | 8,8                  |
|   | <i>Итого по дисциплине:</i>                                                     |                  | 32                |    | 32 | 32,8                 |

**Курсовые работы:** предусмотрена.

#### Примерная тематика курсовых работ (проектов)

1. Построение полей разложений многочленов над конечными полями
2. Деревья и их автоморфизмы
3. Алгоритм извлечения квадратного корня по простому модулю
4. Линейные регистры сдвига с обратной связью
5. Коды Хэмминга и сжатие информации
6. Реляционные алгебры
7. Коммерческие продукт, реализующие модель распределенных баз данных

8. Решение квадратных уравнений в конечных полях с использованием логарифмов Якоби
9. Обзор популярных БЧХ-кодов
10. Недостатки модели Белла-ЛаПадула.

**Форма проведения аттестации по дисциплине: зачет**

**Основная литература:**

1. Бирюков А.А. Информационная безопасность: защита и нападение, 2-е изд. [Электронный ресурс]. – М.: ДМК Пресс, 2017. – URL: <http://e.lanbook.com/view/book/93278/>
2. Галатенко В.А. Стандарты информационной безопасности, 2-е изд. – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2016, 308 с.
3. Нестеров С.А. Основы информационной безопасности, 4-е изд. [Электронный ресурс]. – СПб.: Лань, 2018. – <https://e.lanbook.com/book/103908>.

**Дополнительная литература:**

1. Шаньгин В.Ф. Информационная безопасность. [Электронный ресурс]. – М.: ДМК Пресс, 2014. – URL: <http://e.lanbook.com/view/book/50578/>
2. Водяхо А.И., Выговский Л.С., Дубенецкий В.А., Цехановский В.В. Архитектурные решения информационных систем, 2-е изд. [Электронный ресурс]. – М.: Лань, 2017. – URL: [https://e.lanbook.com/book/96850?category\\_pk=1537#authors](https://e.lanbook.com/book/96850?category_pk=1537#authors).
3. Рассолов М.М. Информационное право. [Электронный ресурс]. – М.: Проспект, 2015. – URL: <http://e.lanbook.com/view/book/54523/>

**Интернет-ресурсы:**

1. Пакет компьютерной алгебры Sage 8.2. Официальный сайт <http://sagemath.org/>
2. Пакет компьютерной алгебры Gap4r9p1. Официальный сайт <http://www.gap-system.org/>
3. Пакет компьютерной алгебры PARI/GT 2.9. Официальный сайт <http://pari.math.u-bordeaux.fr/>
4. Пакет компьютерной алгебры Maple 2018. <http://www.maplesoft.com>
5. <http://www.pravo.gov.ru> – официальный портал правовой информации
6. <http://www.government.ru> - интернет-портал Правительства РФ
7. <http://graph.document.kremlin.ru> - раздел «Документы» портала Президента России
8. <http://minsvyaz.ru/ru> - сайт Минкомсвязи РФ
9. <http://www.rsoc.ru> - сайт Федеральной службы Роскомнадзор
10. <http://www.scrf.gov.ru> – сайт Совета безопасности РФ
11. <http://base.consultant.ru> – сайт правовой информации «Консультант+»
12. <http://www.fstec.ru> – официальный сайт ФСТЭК России
13. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru/>)
14. Электронная библиотека <http://gen.lib.rus.ec/>

Автор РПД

Рожков А.В.