

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Щёкина Вера Викторовна  
Должность: Ректор  
Дата подписания: 10.05.2019 12:06  
Уникальный программный идентификатор:  
a2232a55157e576571a8999b1190892a753989420420556b01575a454e57789



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Благовещенский государственный педагогический университет»**

**ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА  
Рабочая программа дисциплины**

**УТВЕРЖДАЮ**

**И.о. декана физико-математического  
факультета ФГБОУ ВО «БГПУ»**

**О.А.Днепровская  
«22» мая 2019 г.**

**Рабочая программа дисциплины  
ОСНОВЫ КРИПТОГРАФИИ**

**Направление подготовки**

**02.03.03 – МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ И  
АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ**

**Профиль**

**ТЕХНОЛОГИЯ ПРОГРАММИРОВАНИЯ**

**Уровень высшего образования  
БАКАЛАВРИАТ**

**Принята  
на заседании кафедры физического  
и математического образования  
(протокол № 9 от «15» мая 2019 г.)**

**Благовещенск 2019**

## СОДЕРЖАНИЕ

|                                                                                                               |           |
|---------------------------------------------------------------------------------------------------------------|-----------|
| <b>1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА .....</b>                                                                          | <b>3</b>  |
| <b>2 УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ .....</b>                                                               | <b>4</b>  |
| <b>3 СОДЕРЖАНИЕ ТЕМ (РАЗДЕЛОВ) .....</b>                                                                      | <b>5</b>  |
| <b>4 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ (УКАЗАНИЯ) ДЛЯ СТУДЕНТОВ ПО<br/>ИЗУЧЕНИЮ ДИСЦИПЛИНЫ .....</b>                  | <b>6</b>  |
| <b>5 ПРАКТИКУМ ПО ДИСЦИПЛИНЕ .....</b>                                                                        | <b>8</b>  |
| <b>6 ДИДАКТИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ КОНТРОЛЯ (САМОКОНТРОЛЯ)<br/>УСВОЕННОГО МАТЕРИАЛА.....</b>                    | <b>8</b>  |
| <b>7 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ .....</b>                                               | <b>20</b> |
| <b>В ПРОЦЕССЕ ОБУЧЕНИЯ .....</b>                                                                              | <b>20</b> |
| <b>8 ОСОБЕННОСТИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ ИНВАЛИДАМИ И ЛИЦАМИ С<br/>ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ .....</b> | <b>20</b> |
| <b>9 СПИСОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ .....</b>                                                    | <b>21</b> |
| <b>10 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА .....</b>                                                                  | <b>21</b> |
| <b>11 ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ .....</b>                                                                   | <b>23</b> |

## 1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

**1.1 Цель дисциплины:** обучение студентов, специализирующихся в области информационных систем, основам криптографии, позиционированию общематематических подходов к информационным технологиям, а также применению полученных знаний и навыков к решению ряда профессиональных задач.

**1.2 Место дисциплины в структуре ООП:** Дисциплина «Основы криптографии» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1 (Б.1. В.ДВ.01.01). Преподавание дисциплины связано с другими дисциплинами учебного плана: «Алгебра и теория чисел», «Математический анализ».

**1.3 Дисциплина направлена на формирование следующих компетенций:** ОПК-2, ПК-8:

- **ОПК-2.** Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности, **индикаторами** достижения которой является:

- ОПК-2.1 - **знает:** математические основы программирования и языков программирования, организации баз данных и компьютерного моделирования; математические методы оценки качества, надежности и эффективности программных продуктов; математические методы организации информационной безопасности при разработке и эксплуатации программных продуктов и программных комплексов;

- ОПК-2.2 – **умеет:** использовать этот аппарат в профессиональной деятельности;

- ОПК-2.3 – **имеет навыки:** применения данного математического аппарата при решении конкретных задач.

- **ПК-8.** Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования.

- ПК-8.1. Знает современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования.

- ПК-8.2. Умеет разрабатывать и реализовывать алгоритмы математических моделей на базе языков и пакетов прикладных программ моделирования.

- ПК-8.3. Имеет практический опыт разработки и реализации алгоритмов их на базе языков и пакетов прикладных программ моделирования.

### 1.4 Перечень планируемых результатов обучения.

**В результате изучения дисциплины студент должен**

**знать:**

- Основные криптосистемы;
- Математическое обоснование криптографии.

**уметь:**

- применять криптосистему Хилла;
- применять криптосистему Меркля-Хелмана;
- применять криптосистему Месси-Омуры;
- применять криптосистему Диффи-Хелмана;
- применять криптосистему DES;
- применять криптосистему ГОСТ 28147-89.

**владеть:**

– навыками практического использования аппарата дисциплины при решении конкретных задач.

**1.5 Общая трудоемкость дисциплины «Основы криптографии»** составляет 3 зачетные единицы (далее – ЗЕ) (108 часов):

Программа предусматривает изучение материала на лекциях и лабораторных занятиях. Предусмотрена самостоятельная работа студентов по темам и разделам. Проверка знаний осуществляется фронтально, индивидуально.

#### **1.6 Объем дисциплины и виды учебной деятельности**

##### **Объем дисциплины и виды учебной деятельности (очная форма обучения)**

| Вид учебной работы      | Всего часов | Семестр |
|-------------------------|-------------|---------|
|                         |             | 5       |
| Общая трудоемкость      | 108         | 108     |
| Аудиторные занятия      | 60          | 60      |
| Лекции                  | 24          | 24      |
| Практические занятия    | 36          | 36      |
| Самостоятельная работа  | 48          | 48      |
| Вид итогового контроля: |             | зачет   |