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

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