



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

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»**

А.В. Василенко

«23» марта 2016 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 № 7 от «23» марта 2016 г.)**

Благовещенск 2016

Рабочая программа дисциплины разработана на основе:

- ФГОС ВО по направлению подготовки 02.03.03 «Математическое обеспечение и администрирование информационных систем» (квалификация (степень) «бакалавр»), утверждённого Министерством образования и науки РФ от 12 марта 2015 г. № 222.
- Учебного плана по профилю «Технологии программирования», утвержденного Ученым советом БГПУ от «23» марта 2016 г. Протокол № 6.
- Приказа Министерства образования и науки РФ № 1367 от 19.12.2013 г. «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры».

Разработчик рабочей программы – доцент кафедры физического и математического образования, к. ф.-м. н. П.П. Алутин.

СОДЕРЖАНИЕ

<i>1 Пояснительная записка</i>	4
1.1 Цель и задачи освоения учебной дисциплины:	4
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.....	4
1.2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП.	4
1.3 Место дисциплины в структуре ООП:.....	4
1.4 Объем дисциплины и виды учебной работы.....	4
<i>2 Учебно-тематический план</i>	5
2.1 Интерактивное обучение по дисциплине	5
<i>3 Содержание разделов дисциплины</i>	6
<i>4 Методические рекомендации для студентов для изучения дисциплины</i>	7
<i>5 Практикум по дисциплине</i>	8
5.1 План практических занятий.....	8
<i>6 Дидактические материалы для контроля (самоконтроля) усвоенного материала</i>	10
6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины	10
6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания по дисциплине	14
6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения дисциплины	15
Самостоятельные и контрольные работы	15
Программа зачета	17
6.4 Методические материалы, определяющие процедуру оценивания знаний, умений и навыков	18
Процедура оценивания.....	18
<i>7 Перечень информационных технологий, используемых в процессе обучения</i>	19
<i>8 Список литературы и информационных ресурсов</i>	19
8.1 Основная.....	19
8.2 Дополнительная	19
8.3 Информационные ресурсы	19
<i>9 Материально-техническая база</i>	20
<i>10 Лист изменений и дополнений</i>	20

1 Пояснительная записка

1.1 Цель и задачи освоения учебной 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 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП.

Процесс изучения дисциплины «Основы криптографии» направлен на формирование следующих общепрофессиональных компетенций:

- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1);
- способность применять в профессиональной деятельности знания математических основ информатики (ОПК-2);
- способность использовать знания методов проектирования и производства программного продукта, принципов построения, структуры и приемов работы с инструментальными средствами, поддерживающими создание программного обеспечения (ПО) (ОПК-8);
- способность использовать навыки выбора, проектирования, реализации, оценки качества и анализа эффективности программного обеспечения для решения задач в различных предметных областях (ОПК-11).

В результате изучения дисциплины студент должен

знать:

- основные криптосистемы;
- математическое обоснование криптографии;

уметь:

- применять криптосистему Диффи-Хелмана;
- применять криптосистему RSA;
- применять алгоритмы полиномиальной арифметики.

владеть:

- классическими знаниями дисциплины «Основы криптографии»;
- навыками практического использования аппарата дисциплины при решении конкретных задач.

1.3 Место дисциплины в структуре ООП:

Дисциплина «Основы криптографии» (Б1.В.ДВ.5.1) относится к дисциплинам по выбору вариативной части Блока 1 дисциплин (модулей) основной образовательной программы бакалавриата по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем. Для освоения дисциплины используются знания, умения и виды деятельности, сформированные в процессе изучения математических дисциплин на предыдущем уровне образования.

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа).

1.4 Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		4
Общая трудоемкость	72	72
Аудиторные занятия	40	40
Лекции	18	18
Лабораторные работы		
Практические занятия	22	22
Самостоятельная работа	32	32
Вид итогового контроля:		зачет