

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**федеральное государственное автономное  
образовательное учреждение высшего образования  
«Национальный исследовательский Нижегородский государственный университет  
им. Н.И. Лобачевского»**

Институт информационных технологий, математики и механики

---

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

**Рабочая программа дисциплины**

Современная криптография

---

Уровень высшего образования

Магистратура

---

Направление подготовки / специальность

01.04.02 - Прикладная математика и информатика

---

Направленность образовательной программы

Компьютерные науки и приложения

---

Форма обучения

очная

---

г. Нижний Новгород

2024 год начала подготовки

## 1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.ДВ.06.01 Современная криптография относится к части, формируемой участниками образовательных отношений образовательной программы.

## 2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции		Наименование оценочного средства	
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	Для текущего контроля успеваемости	Для промежуточной аттестации
ПК-11: Способен разрабатывать и анализировать концептуальные и теоретические модели решаемых задач производственно-технологической деятельности	ПК-11.1: Знает методы разработки и анализа концептуальных теоретических моделей решаемых производственно-технологических задач. ПК-11.2: Умеет применять методы разработки и анализа концептуальных теоретических моделей решаемых производственно-технологических задач. ПК-11.3: Имеет навыки применения методов разработки и анализа концептуальных теоретических моделей решаемых производственно-технологических задач.	ПК-11.1: Знает методы разработки и анализа криптографических алгоритмов и протоколов.  ПК-11.2: Умеет применять методы разработки и анализа криптографических алгоритмов и протоколов.  ПК-11.3: Имеет навыки применения и анализа криптографических алгоритмов и протоколов.	Сообщение на семинарских занятиях	Зачёт: Контрольные вопросы
ПК-4: Способен разрабатывать и анализировать концептуальные и теоретические модели решаемых научных проблем и задач	ПК-4.1: Знает методы разработки и анализа концептуальных теоретических моделей решаемых научных проблем и задач ПК-4.2: Умеет применять методы разработки и анализа концептуальных теоретических моделей решаемых научных проблем и задач ПК-4.3: Имеет навыки применения методов	ПК-4.1: Знает методы разработки и анализа криптографических алгоритмов  ПК-4.2: Умеет применять методы разработки и анализа криптографических алгоритмов  ПК-4.3: Имеет навыки применения методов разработки	Сообщение на семинарских занятиях	Зачёт: Контрольные вопросы

	разработки и анализа концептуальных теоретических моделей решаемых научных проблем и задач	и анализа криптографических алгоритмов.		
--	--	--	--	--

### 3. Структура и содержание дисциплины

#### 3.1 Трудоемкость дисциплины

	<b>очная</b>
<b>Общая трудоемкость, з.е.</b>	<b>3</b>
<b>Часов по учебному плану</b>	<b>108</b>
в том числе	
<b>аудиторные занятия (контактная работа):</b>	
- занятия лекционного типа	<b>16</b>
- занятия семинарского типа (практические занятия / лабораторные работы)	<b>16</b>
- КСР	<b>1</b>
<b>самостоятельная работа</b>	<b>75</b>
<b>Промежуточная аттестация</b>	<b>0</b> <b>Зачёт</b>

#### 3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

Наименование разделов и тем дисциплины	Всего (часы)	в том числе			
		Контактная работа (работа во взаимодействии с преподавателем), часы из них			Самостоятельная работа обучающегося, часы
		Занятия лекционного типа	Занятия семинарского типа (практические занятия/ лабора торные работы), часы	Всего	
	Ф Ф Ф	Ф Ф Ф	Ф Ф Ф	Ф Ф Ф	Ф Ф Ф
Вычисления в кольце целых чисел и в конечных полях.	50	10	8	18	32
Криптосистемы с открытым ключом	42	4	6	10	32
Криптографические протоколы	15	2	2	4	11
Аттестация	0				
КСР	1			1	
Итого	108	16	16	33	75

#### Содержание разделов и тем дисциплины

1. Классические алгоритмы арифметических операций.
2. Умножение методом Карацубы.

3. Деление методом Ньютона.
4. Дихотомические алгоритмы возведения в степень.
5. Расширенный алгоритм Евклида нахождения НОД.
6. Расширенный бинарный алгоритм нахождения НОД.
7. Быстрое преобразование Фурье.
8. Умножение целых чисел с помощью быстрого преобразования Фурье.
9. Непрерывные дроби.
10. Квадратичные вычеты.
11. Нахождение больших простых чисел.
12. Факторизация целых чисел.
13. Дискретный логарифм.
14. Метод Соловея–Штрассена проверки простоты числа.
15. Метод Миллера–Рабина проверки простоты числа.
16. Система RSA.
17. Криптосистема Эль Гамала.
18. Криптографические протоколы

#### **4. Учебно-методическое обеспечение самостоятельной работы обучающихся**

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

Лекции по криптографии.

#### **5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)**

##### **5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:**

##### **5.1.1 Типовые задания (оценочное средство - Сообщение на семинарских занятиях) для оценки сформированности компетенции ПК-11:**

1. Классические алгоритмы арифметических операций.
2. Умножение методом Карацубы.
3. Деление методом Ньютона.
4. Дихотомические алгоритмы возведения в степень.
5. Расширенный алгоритм Евклида нахождения НОД.
6. Расширенный бинарный алгоритм нахождения НОД.
7. Быстрое преобразование Фурье.
8. Умножение целых чисел с помощью быстрого преобразования Фурье.
9. Непрерывные дроби.
10. Квадратичные вычеты.
11. Нахождение больших простых чисел.
12. Факторизация целых чисел.
13. Дискретный логарифм.
14. Метод Соловея–Штрассена проверки простоты числа.
15. Метод Миллера–Рабина проверки простоты числа.
16. Система RSA.

17. Криптосистема Эль Гамала.
18. Криптографические протоколы

### 5.1.2 Типовые задания (оценочное средство - Сообщение на семинарских занятиях) для оценки сформированности компетенции ПК-4:

1. Классические алгоритмы арифметических операций.
2. Умножение методом Карацубы.
3. Деление методом Ньютона.
4. Дихотомические алгоритмы возведения в степень.
5. Расширенный алгоритм Евклида нахождения НОД.
6. Расширенный бинарный алгоритм нахождения НОД.
7. Быстрое преобразование Фурье.
8. Умножение целых чисел с помощью быстрого преобразования Фурье.
9. Непрерывные дроби.
10. Квадратичные вычеты.
11. Нахождение больших простых чисел.
12. Факторизация целых чисел.
13. Дискретный логарифм.
14. Метод Соловея–Штрассена проверки простоты числа.
15. Метод Миллера–Рабина проверки простоты числа.
16. Система RSA.
17. Криптосистема Эль Гамала.
18. Криптографические протоколы

### Критерии оценивания (оценочное средство - Сообщение на семинарских занятиях)

Оценка	Критерии оценивания
зачтено	Достаточно полное изложение материала, отсутствие грубых ошибок.
не зачтено	Поверхностное знание материала, хотя бы одна грубая ошибка.

### 5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

#### Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатор достижения компетенций)	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				
<u>Знания</u>	Отсутствие знаний теоретического материала.	Уровень знаний ниже минимальных требований.	Минимально допустимый уровень	Уровень знаний в объеме, соответствующему	Уровень знаний в объеме, соответствующему	Уровень знаний в объеме, соответствующему	Уровень знаний в объеме, превышающему

	Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Имели место грубые ошибки	знаний. Допущено много негрубых ошибок	ющем программе подготовки . Допущено несколько негрубых ошибок	ющем программе подготовки . Допущено несколько несущественных ошибок	ующем программе подготовк и. Ошибок нет.	м программу подготовки.
<u>Умения</u>	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи с отдельным и несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие базовых навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторым и недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторым и недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрирован творческий подход к решению нестандартных задач

### Шкала оценивания при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	<b>превосходно</b>	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне выше предусмотренного программой
	<b>отлично</b>	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично».
	<b>очень хорошо</b>	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
	<b>хорошо</b>	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо».
	<b>удовлетворительно</b>	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»

<b>не зачтено</b>	<b>неудовлетворительно</b>	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
	<b>плохо</b>	Хотя бы одна компетенция сформирована на уровне «плохо»

### **5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:**

#### **5.3.1 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПК-11**

1. Классические алгоритмы арифметических операций.
2. Умножение методом Карацубы.
3. Деление методом Ньютона.
4. Дихотомические алгоритмы возведения в степень.
5. Расширенный алгоритм Евклида нахождения НОД.
6. Расширенный бинарный алгоритм нахождения НОД.
7. Быстрое преобразование Фурье.
8. Умножение целых чисел с помощью быстрого преобразования Фурье.
9. Непрерывные дроби.
10. Квадратичные вычеты.
11. Нахождение больших простых чисел.
12. Факторизация целых чисел.
13. Дискретный логарифм.
14. Метод Соловея–Штрассена проверки простоты числа.
15. Метод Миллера–Рабина проверки простоты числа.
16. Система RSA.
17. Криптосистема Эль Гамала.
18. Криптографические протоколы

#### **5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПК-4**

1. Классические алгоритмы арифметических операций.
2. Умножение методом Карацубы.
3. Деление методом Ньютона.
4. Дихотомические алгоритмы возведения в степень.
5. Расширенный алгоритм Евклида нахождения НОД.
6. Расширенный бинарный алгоритм нахождения НОД.
7. Быстрое преобразование Фурье.
8. Умножение целых чисел с помощью быстрого преобразования Фурье.
9. Непрерывные дроби.
10. Квадратичные вычеты.
11. Нахождение больших простых чисел.
12. Факторизация целых чисел.
13. Дискретный логарифм.
14. Метод Соловея–Штрассена проверки простоты числа.
15. Метод Миллера–Рабина проверки простоты числа.

16. Система RSA.
17. Криптосистема Эль Гамала.
18. Криптографические протоколы

### **Критерии оценивания (оценочное средство - Контрольные вопросы)**

Оценка	Критерии оценивания
зачтено	Компетенции ПК-4 и ПК-11 сформированы на уровне не ниже «удовлетворительно»
не зачтено	Уровень формирования компетенций ПК-4 и ПК-11 оценивается как «неудовлетворительно»

### **6. Учебно-методическое и информационное обеспечение дисциплины (модуля)**

Основная литература:

1. Василенко Олег Николаевич. Теоретико-числовые алгоритмы в криптографии / МГУ, Ин-т проблем информ. безопасности. - М. : МНИЦМО, 2003. - 328 с. - (Информационная безопасность. Криптография). - ISBN 5-94057-103-4 : 37.00., 2 экз.
2. Введение в криптографию : Новые математические дисциплины / под ред. В. В. Яценко. - СПб. : Питер, 2001. - 288 с. : ил. - ISBN 5-318-00443-1 : 74.36., 2 экз.

Дополнительная литература:

1. Введение в теоретико-числовые методы криптографии / Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. - Санкт-Петербург : Лань, 2022. - 400 с. - Допущено УМО вузов по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности «Криптография». - Книга из коллекции Лань - Информатика. - ISBN 978-5-8114-1116-0., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=799760&idb=0>.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

Изд-во Лань (<https://e.lanbook.com/book>)

### **7. Материально-техническое обеспечение дисциплины (модуля)**

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.



Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки 01.04.02 - Прикладная математика и информатика.

Автор(ы): Веселов Сергей Иванович, кандидат физико-математических наук, доцент.

Заведующий кафедрой: Золотых Николай Юрьевич, доктор физико-математических наук.

Программа одобрена на заседании методической комиссии от 13.12.2023, протокол № 3.