

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Физический факультет

---

УТВЕРЖДЕНО

решением Ученого совета ННГУ

протокол № 12 от 09.11.2022 г.

**Рабочая программа дисциплины**

Информационная безопасность и защита информации

---

Уровень высшего образования

Бакалавриат

---

Направление подготовки / специальность

09.03.02 - Информационные системы и технологии

---

Направленность образовательной программы

Информационные технологии в системах космической связи

---

Форма обучения

очная

---

г. Нижний Новгород

2022 год начала подготовки

## 1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.1.07 Информационная безопасность и защита информации 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-16: Способен к выполнению работ по проектированию, отладке, проверке работоспособности и модификации программного обеспечения информационных систем	ПК-16.1: Знать методы разработки программного обеспечения и технологии программирования ПК-16.2: Владеть навыками проектирования, отладки программного обеспечения и проверки работоспособности	ПК-16.1: Знать математический аппарат, необходимый для анализа и разработки криптографических систем защиты информации, система защиты целостности данных. Знать основные концепции защиты информации. Знать простейшие протоколы симметричного и асимметричного шифрования данных, защиты целостности информации. Знать основные типы методов шифрования информации и возможности их применения в различных сферах.  ПК-16.2: Уметь решать типовые учебные задачи по основным разделам теории чисел, арифметики по модулю. Уметь реализовывать простейшие алгоритмы криптографической защиты информации. Уметь соблюдать основные требования к информационной безопасности в Российской Федерации. Уметь составлять алгоритмы реализации	Практическое задание	Зачёт: Тест

		<p>простейших протоколов защиты информации.</p> <p>Уметь применять знания протоколов криптографической защиты информации, протоколов защиты целостности персональных данных в задачах разработки и администрирования инфокоммуникационных систем и сетей.</p>		
--	--	---	--	--

### 3. Структура и содержание дисциплины

#### 3.1 Трудоемкость дисциплины

	очная
<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	32
- занятия семинарского типа (практические занятия / лабораторные работы)	32
- КСР	1
<b>самостоятельная работа</b>	<b>43</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/лабораторные работы), часы	Всего	
	0 0	0 0	0 0	0 0	0 0
Основные задачи защиты информации. Классификация систем защиты информации	5	4	0	4	1
Криптографические методы защиты информации. Основные определения и краткая история развития криптографии	5	4	0	4	1
Математические основы криптографии	5	4	0	4	1

Криптографические алгоритмы с симметричными ключами	5	4	0	4	1
Реализация алгоритма DES	32	4	16	20	12
Криптографические алгоритмы с несимметричными ключами	5	4	0	4	1
Реализация алгоритма RSA	24	4	8	12	12
Методы защиты целостности данных	5	4	0	4	1
Индивидуальное практическое задание	21	0	8	8	13
Аттестация	0				
КСР	1			1	
Итого	108	32	32	65	43

### Содержание разделов и тем дисциплины

Основные задачи защиты информации. Классификация систем защиты информации

Криптографические методы защиты информации. Основные определения и краткая история развития криптографии

Математические основы криптографии

Криптографические алгоритмы с симметричными ключами

Реализация алгоритма DES

Криптографические алгоритмы с несимметричными ключами

Реализация алгоритма RSA

Методы защиты целостности данных

#### 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.

Самостоятельная работа студентов включает изучение учебных и учебно-методических пособий, лекционного материала по соответствующим разделам дисциплины, в том числе с использованием систем компьютерной графики и электронных образовательных ресурсов. Одной из основных задач самостоятельной работы является подготовка к реализации численных алгоритмов модульной арифметики и выполнению моделирующих компьютерных программ.

#### 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 - Практическое задание) для оценки сформированности компетенции ПК-16:**

Создать приложение с графическим интерфейсом на языке программирования C++/C#, осуществляющее шифрование и расшифрование текста по алгоритму DES.

Создать приложение с графическим интерфейсом на языке C++/C#, реализующее алгоритм шифрования и расшифрования текста по алгоритму RSA.

Создать приложение на языке C++/C#, позволяющее генерировать электронную цифровую подпись введенного текста произвольной длины и осуществлять проверку подписи на основе алгоритма DSA.

### Критерии оценивания (оценочное средство - Практическое задание)

Оценка	Критерии оценивания
зачтено	Практическое задание выполнено в полном объеме. Допускаются незначительные ошибки, исправленные после замечания преподавателя.
не зачтено	Практическое задание выполнено не в полном объеме. Допущены ошибки, которые не удалось исправить после замечания преподавателя.

## 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. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Ошибок нет.	Уровень знаний в объеме, превышающем 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	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, выполнен	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

				недочетами		ы все задания в полном объеме	
<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	превосходно	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
	отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично».
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо».
	удовлетворительно	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»
не зачтено	неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
	плохо	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 - Тест) для оценки сформированности компетенции ПК-16

1. Вероятностным тестом на простоту числа является тест. (1 балл)

1) Агравала      2) Люка      3) Миллера      4) Ферма

2. Дополните предложение – вместо **X** впишите формулу. Согласно малой теореме Ферма, если число - простое, то для любого натурального числа выполняется соотношение **X**. (2 балла)

## Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
зачтено	В тесте набрано больше половины от максимально возможного количества баллов
не зачтено	В тесте набрано не больше половины от максимально возможного количества баллов

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

Основная литература:

1. Основы современной криптографии и стеганографии / Рябко Б.Я., Фионов А.Н. - Москва : Горячая линия - Телеком, 2013., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=646239&idb=0>.
2. Романьков Виталий Анатольевич. Введение в криптографию : Курс лекций / Омский государственный университет им. Ф.М. Достоевского. - 2. - Москва : Издательство "ФОРУМ", 2023. - 240 с. - ВО - Бакалавриат. - ISBN 978-5-00091-493-9. - ISBN 978-5-16-105918-0. - ISBN 978-5-16-013395-9., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=837662&idb=0>.
3. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты / Фомичёв В. М., Мельников Д. А. ; под ред. Фомичёва В.М. - Москва : Юрайт, 2022. - 209 с. - (Высшее образование). - URL: <https://urait.ru/bcode/489745> (дата обращения: 05.01.2022). - ISBN 978-5-9916-7088-3 : 699.00. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=789056&idb=0>.
4. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. - Москва : Юрайт, 2022. - 245 с. - (Высшее образование). - URL: <https://urait.ru/bcode/490421> (дата обращения: 14.08.2022). - ISBN 978-5-9916-7090-6 : 1009.00. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=816780&idb=0>.

Дополнительная литература:

1. Теоретико-численные методы в криптографии / Кнауб Л.В., Новиков Е.А., Шитов Ю.А. - Москва : СФУ, 2011., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=655905&idb=0>.

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

-

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

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами, специализированным оборудованием: в том числе,

- высокотехнологичным оборудованием: серверная вычислительная техника, включая сервера и АРМы Гравитон, серверные шкафы, программно-аппаратные комплексы, сетевое оборудование;
- вычислительными ресурсами: терминал-классы с 26 стационарными и 3 мобильными рабочими местами на базе современных ПК с лицензионным программным обеспечением;
- офисным и мультимедийным оборудованием, включая проектор, экран и ТВ-панель, специализированная мебель.

Перечисленное выше оборудование входит в состав Учебно-лабораторного интерактивного комплекса "Распределенные вычисления" для проведения занятий для студентов с использованием современной вычислительной техники при обучении моделированию, проектированию и разработке распределенных вычислительных комплексов и проведения практических занятий по дисциплинам, предусмотренных программой.

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/специальности 09.03.02 - Информационные системы и технологии.

Автор(ы): Чуманкин Юрий Евгеньевич.

Заведующий кафедрой: Морозов Олег Александрович, доктор физико-математических наук.

Программа одобрена на заседании методической комиссии от 20.01.2022, протокол № б/н.