МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Радиофизический факультет
(факультет / институт / филиал)

УТВЕРЖДЕНО
решением президиума
Ученого совета ННГУ
протокол от
«30» ноября 2022 г. № 13

Рабочая программа дисциплины

Математические основы защиты информации
(наименование дисциплины (модуля)

Уровень высшего образования
магистратура
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
02.04.02 «Фундаментальная информатика и информационные технологии»
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Теория информации
(указывается профиль / магистерская программа / специализация)

Форма обучения
очная
(очная / очно-заочная / заочная)

Нижний Новгород

2023 год

1. Место дисциплины в структуре ООП

Дисциплина Б1.О.01 «Математические основы защиты информации и информационной безопасности» относится к части ООП направления подготовки 02.04.02 Фундаментальная информатика и информационные технологии, формируемой участниками образовательных отношений.

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**	
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает структуру жизненного цикла проекта.	*Знать* структуру жизненного цикла проекта применительно к цифровой обработке сигналов *Уметь* Определять этап жизненного цикла, на котором проект находится на данном этапе применительно к цифровой обработке сигналов *Владеть* навыком принятия решения на любом этапе жизненного цикла проекта	*Письменные и устные ответы на опросы, практическое контрольное задание в виде проекта, письменные и устные ответы на теоретические вопросы, решение практических задач.*
	УК-2.2. Умеет адаптировать жизненный цикл под специфику конкретных проектов.	*Знать* основные требования к составлению проекта жизненного цикла проекта *Уметь* организовывать жизненный цикл	

		проекта применительно к цифровой обработке сигналов *Владеть* Навыками оценки полученных результатов и формулировки выводов о проделанной работе	
	УК-2.3. Владеет методами управления проектом на всех этапах его жизненного цикла.	*Знать* методы управления проектом *Уметь* определять этап жизненного цикла проекта *Владеть* методами управления проектом на всех этапах его жизненного цикла	
ОПК-4. Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1. Знает принципы сбора и анализа информации, создания информационных систем на стадиях жизненного цикла.	*Знать* принципы сбора и анализа информации, создания информационных систем на стадиях жизненного цикла *Уметь* различать стадии жизненного цикла проекта *Владеть* навыком создания информационных систем на разных стадиях жизненного цикла	*Письменные и устные ответы на опросы, практическое контрольное задание в виде проекта, письменные и устные ответы на теоретические вопросы, решение практических задач.*
	ОПК-4.2. Умеет осуществлять управление проектами информационных систем.	*Знать* требования по информационной безопасности *Уметь* осуществлять управление проектами информационных систем	

		Владеть навыком решения задач в области профессиональной деятельности с учетом требований по информационной безопасности	
	ОПК-4.3. Имеет практический опыт анализа и интерпретации информационных систем.	*Знать* информационно-коммуникационные технологии для решения задач *Уметь* анализировать собранную информацию *Владеть* практическим опытом анализа и интерпретации информационных систем	

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения
Общая трудоемкость	**4 ЗЕТ**
Часов по учебному плану	**108**
в том числе	
аудиторные занятия (контактная работа): **- занятия лекционного типа** **- занятия семинарского типа (практические занятия / лабораторные работы)**	**32**
самостоятельная работа	**75**
КСР	**1**
Промежуточная аттестация – зачет	

Содержание дисциплины (модуля)

Наименование и краткое содержание разделов и тем дисциплины (модуля), **форма промежуточной аттестации по дисциплине (модулю)**	**Всего (часы)**		В том числе											
			Контактная работа (работа во взаимодействии с преподавателем), часы из них										**Самостоятельная работа**	
			Занятия лекционного типа		**Занятия семинарского типа**		**Занятия лабораторного типа**		**Консультации**		**Всего**			
	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная
Тема 1. История развития криптографии. Основные понятия.	7		2		0		0		0		2		5	
Тема 2. Математические основы криптографии.	50		15		0		0		0		15		35	
Тема 3. Хеш-функции	50		15		0		0		0		15		35	
В том числе текущий контроль	1		0		1		0		0		1		0	
Промежуточная аттестация - **Зачет**														

В соответствии с рабочей программой и тематическим планом изучение дисциплины проходит в виде аудиторной и самостоятельной работы студентов. Учебный процесс в аудитории осуществляется в форме практических занятий.

Образовательные технологии, способствующие формированию компетенций
используемые на занятиях лекционного типа:

- лекции с проблемным изложением учебного материала;
- лекции с детальным объяснением нового материала и его связи с уже пройденным материалом.

На лекциях раскрываются следующие основные темы изучаемого курса, которые входят в рабочую программу:

Основные понятия криптографии. Стойкость шифров. Теоретическая и практическая стойкость криптосистем. Обобщенная схема для криптосистем с закрытыми ключами шифрования. Основные исторические этапы становления криптографии. Криптографические и стеганографические методы защиты информации. Основы криптоанализа. История создания частотного анализа. Одноалфавитный шифр. Многоалфавитные шифры. Омофонический шифр замены. Диграф. Великий шифр. Шифр Билля. Шифр Виженера. Взлом шифра Виженера.

Раздел 2. Математические основы криптографии

Понятие вычета по модулю. Понятие сравнимости двух чисел. Введение в конечные поля. Понятие группы. Операции в группах. Кольцо. Поле. Поле Галуа. Неприводимые многочлены. Простые числа. Утверждение о сравнимости чисел. Понятие обратного числа. Мультипликативность функции. Китайская теорема об остатках. Теорема Ферма. Функция Эйлера. Теорема Эйлера. Алгоритм Евклида. Расширенный алгоритм Евклида. Показатели и первообразные корни. Дискретные логарифмы. Генераторы случайных чисел. Проверка качества работы ГСЧ. Преобразование Уолша-Адамара. Эллиптические кривые. Тесты числа на простоту. Принципы построения больших простых чисел. Алгоритм Адлемана-Ленстры. Разложение составных чисел на множители.

Раздел 3. Хеш-функции

Понятие хеш-функции. Коллизия. Хеш-функции Наорра и Юнга. Проверка целостности информации с использованием хеш-функций. Нахождение коллизий хеш-функций в общем случае. Парадокс о днях рождения. Атака «встреча посередине» для хеш-функций. Линейное разделение секрета.

Формой **итогового контроля** знаний студентов по дисциплине является **зачет**, в ходе которого оценивается уровень теоретических знаний, навыки применения алгоритмов и методы их анализа.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Используются виды самостоятельной работы студента: в читальном зале библиотеки, в учебных кабинетах (лабораториях), компьютерных классах, с доступом к ресурсам Интернет и в домашних условиях. Порядок выполнения самостоятельной работы соответствует программе курса и контролируется в ходе проведения лекционных занятий и в конце курса при проведении экзамена по данной дисциплине.

Во время лекций формулируются проблемы, которые студенты должны решить самостоятельно. На последующих лекциях проводится открытое обсуждение полученных результатов и даётся правильное решение.

Задания для проведения промежуточной аттестации по итогам освоения дисциплины выдаются студентам заранее. В случае необходимости проводятся индивидуальные консультации.

Самостоятельная работа студентов направлена на проработку лекций и выполнение проекта, а также подготовку к зачету и экзамену по указанной дисциплине. При работе над проектом необходимо помнить, что данная дисциплина тесно связана с написанием программ на языке C++, связанных с применением изученных алгоритмов.

Цель самостоятельной работы - подготовка современного компетентного специалиста и формирование способностей и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Для достижения этой цели необходимо:

1) ознакомиться с соответствующей темой программы изучаемой дисциплины;
2) осмыслить круг изучаемых вопросов и логику их рассмотрения;
3) изучить рекомендованную учебно-методическим комплексом литературу по данной теме;
4) тщательно изучить лекционный материал.

Самостоятельная работа подкрепляется учебно-методическим и информационным обеспечением, включающим рекомендованные учебники и учебно-методические пособия, а также конспекты лекций.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине

включающий**:**

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности компетенций						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				
Знания	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 ошибки.	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, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.
Умения	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 отдельными несущественным недочетами, выполнены все задания в полном объеме.	Продемонстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие владения материалом. 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 некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми 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 оценки при промежуточной аттестации

Оценка		Уровень подготовки
	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

зачтено	**отлично**	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «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», ни одна из компетенций не сформирована на уровне «плохо»
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1. Контрольные вопросы

Примеры контрольных вопросов	*Код компетенции (согласно РПД)*
1. Математические основы криптографии	УК-2
2. Основные понятия криптографии: шифр, алгоритм шифрования, ключ шифрования, криптосистема. Обобщенная схема для криптосистем с закрытыми ключами шифрования.	УК-2
3. Основные исторические этапы становления криптографии. Криптографические и стеганографические методы защиты информации. Криптология, криптография и криптоанализ.	УК-2
4. Основы криптоанализа. Определение. История создания частотного анализа. Попытки совершенствования одноалфавитного шифра.	УК-2
5. Многоалфавитные шифры. Омофонический шифр замены. Дифраф. Великий шифр. Шифр Билля.	УК-2
6. Шифр Виженера. Беббидж и его роль во взломе шифра Виженера. Взлом шифра Виженера	УК-2
7. Понятие вычета по модулю. Понятие сравнимости двух чисел.	УК-2
8. Введение в конечные поля. Понятие группы. Циклическая группа. Правила выполнения операций в группах.	УК-2
9. Кольцо. Кольцо с единицей. Подкольцо. Целостное кольцо.	УК-2
10. Поле. Порядок и степень поля. Поле Галуа. Примитивный элемент конечного поля. Неприводимые многочлены. Умножение ненулевых элементов конечного поля.	УК-2
11. Простые числа. Взаимно простые числа. Утверждение о сравнимости чисел. Понятие обратного числа. Утверждение о	УК-2

существовании обратного числа.	
12. Мультипликативность функции.	УК-2
13. Теорема Ферма.	УК-2
14. Функция Эйлера. Функция Мебиуса. Теорема Эйлера.	УК-2
15. Алгоритм Евклида. Расширенный алгоритм Евклида.	УК-2
16. Показатели и первообразные корни.	УК-2
17. Генераторы случайных чисел. Методы построения ГСЧ. Проверка качества работы ГСЧ. Проверка на равномерность распределения. Проверка на статистическую независимость.	УК-2
18. Преобразование Уолша-Адамара. Функции Уолша.	УК-2
19. Эллиптические кривые. Безопасность систем дискретных логарифмов над эллиптическими кривыми.	УК-2
20. Тесты числа на простоту. Принципы построения больших простых чисел.	УК-2
21. Алгоритм Адлемана-Ленстры. Разложение составных чисел на множители.	УК-2
22. Дискретные логарифмы.	УК-2

5.2.2. Контрольные вопросы

Примеры контрольных вопросов	*Код компетенции (согласно РПД)*
1. Нахождение чисел, относящихся к заданному показателю	ОПК-4
2. Система открытого распределения ключей диффи хеллмана:	ОПК-4
3. "Открытое шифрование Эль-Гамаля" 10.1.1	ОПК-4
4. Электронная цифровая подпись Эль-Гамаля	ОПК-4
5. Цифровая подпись Эль-Гамаля с сокращенной длиной параметра s	ОПК-4
6. Вычисление мультипликативно обратных элементов в поле вычетов	ОПК-4
7. Электронная цифровая подпись RSA	ОПК-4
8. открытое распределение ключей с использованием криптосистемы RSA	ОПК-4
9. Слепая подпись Шаума	ОПК-4
10. Система открытого распределения ключей диффи хеллмана:	ОПК-4
11. Цифровая подпись Эль-Гамаля с сокращенной длиной параметра s	ОПК-4

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

а) основная литература:

1. Борисов М. А.; Заводцев И. В.; Чижов И. В.Основы программно-аппаратной защиты информации М. 2013
2. Рябко Б. Я.; Фионов А. Н. Основы современной криптографии и стеганографии
М. 2015
3. Лапонина О. Р. Основы сетевой безопасности: криптографические

алгоритмы и протоколы взаимодействия. М.2011

б) дополнительная литература:

1.Малюк А. А.(2); Пазизин С. В.; Погожин Н. С. Заглавие Введение в защиту информации в автоматизированных системах М. 2001
2. Бабенко Л. К.(3); Курилкина А. М. Заглавие Алгоритмы "распределенных согласований" для оценки вычислительной стойкости криптоалгоритмов
Место издания М. 2008
3.Логачев О. А.; Сальников А. А.(2); Ященко В. В. Булевы функции в теории кодирования и криптологии, М.2004
4.Саймон Сингх, Книга кодов. Тайная история кодов и их взлома, М. 2006.
5. Борисов М. А.; Заводцев И. В.; Чижов И. В.Основы программно-аппаратной защиты информации М. 2013
6. Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев, Криптография. От примитивов к синтезу алгоритмов. С-П. 2004.
7.Сонг Й. Я. Криптоанализ RSA, М. 2011
8. Гашков С. Б.; Применко Э. А.; Черепнев М. А. Криптографические методы защиты информации М. 2010
9. Х.К.А. ван Тилборг, Основы криптологии. Профессиональное руководство и интерактивный учебник, М. «Мир», 2006.

в) программное обеспечение и Интернет-ресурсы.

Visual Studio 8 и выше

6. Материально-техническое обеспечение дисциплины (модуля)

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: мультимедийный проектор.

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 ФГОС ВПО/ВО с учетом рекомендаций и ООП ВПО по направлению **02.04.02 «Фундаментальная информатика и информационные технологии».** (магистратура)

Автор(ы): доцент, Лапинова С.А.

Рецензент (ы): преподаватель Горбунов А.А.

Заведующий кафедрой: д.ф.-м.н., доцент, Дубков А.А.

Программа одобрена на заседании методической комиссии
радиофизического факультета от «14» ноября 2022 года, протокол № 08/22.