

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 / институт / филиал)

УТВЕРЖДЕНО
президиумом Ученого совета ННГУ
протокол от
«31» мая 2023 г. № 6

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
Автоматизация научных исследований
(указывается профиль / магистерская программа / специализация)

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

Нижний Новгород

2023 год

1. Место и цели дисциплины (модуля) в структуре ООП

Дисциплина «Математические основы защиты информации и информационной безопасности» относится к обязательной части Блока Б1 ООП по направлению 02.04.02 – «Фундаментальная информатика и информационные системы», направленность «Теория информации». Трудоемкость дисциплины составляет 3 зачетные единицы. Дисциплина обязательна для освоения в 1 семестре. К моменту изучения дисциплины у студентов присутствуют устойчивые представления, касающиеся понятийного аппарата в области теории алгоритмов, студенты владеют основами алгебры логики, инструментами математического анализа, языком программирования C++.

Целями освоения дисциплины являются:

- Знать основные методы криптографической защиты информации;
- Уметь проводить анализ криптографических алгоритмов на предмет оценки их криптографической устойчивости и эффективности;
- Уметь классифицировать поставленную задачу, выбирать оптимальный метод криптографической защиты для ее решения;
- Знать основные коды, шифры и инструменты для криптографической защиты данных.

Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

Формируемые компетенции (код компетенции, уровень освоения – при наличии в карте компетенции)	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций
УК-2: Способен управлять проектом на всех этапах его жизненного цикла (этап освоения базовый)	УК-2.3. Владеет методами управления проектом на всех этапах его жизненного цикла в области информационной безопасности
ОПК-4: способность использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математики, фундаментальных концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий (этап освоения базовый)	ОПК-4.1. Знает принципы сбора и анализа информации, создания информационных систем на стадиях жизненного цикла в области информационной безопасности

Окончательное завершение формирования компетенций, предусмотренных в рамках данной дисциплины, происходит после сдачи экзамена по этой дисциплине.

2. Структура и содержание дисциплины

Объем дисциплины составляет 3 зачетные единицы, всего 108 часов, из которых 33 часа составляет контактная работа обучающегося с преподавателем (32 часа – занятия лекционного типа, в том числе 1 час - мероприятия текущего контроля успеваемости, и 1

час - мероприятия промежуточной аттестации), 75 часов составляет самостоятельная работа обучающегося.

Содержание дисциплины (модуля)

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

Текущий контроль успеваемости проходит в рамках занятий семинарского и практического типа, групповых или индивидуальных консультаций. Промежуточный контроль осуществляется на зачете. Итоговый контроль осуществляется на экзамене

3. Образовательные технологии

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;

используемые на занятиях практического типа:

- регламентированная самостоятельная деятельность студентов;
- частично-поисковая деятельность при решении задач повышенной сложности,
- текущий контроль знаний студентов с помощью учета посещаемости лекций и работы над проектом к зачету.

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

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.

5. **Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю),**
включающий:

- 6.1. Перечень компетенций выпускников образовательной программы с указанием результатов обучения (знаний, умений, владений), характеризующих этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования

7. УК-2: Способен управлять проектом на всех этапах его жизненного цикла

Индикаторы компетенции	ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ	
	Не зачтено	Зачтено
<u>Знания</u>	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний и выше. Допущенные ошибки не являлись грубыми.
<u>Умения</u>	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи, возможны негрубые ошибки. Выполнены все задания.
Шкала оценок по проценту правильно выполненных контрольных заданий	0 – 30 %	30 – 100 %

ОПК-4: способность использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математики, фундаментальных концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий

Индикаторы компетенции	ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ	
	Не зачтено	Зачтено
<u>Знания</u>	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний и выше. Допущенные ошибки не являлись грубыми.
<u>Умения</u>	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи, возможны негрубые ошибки. Выполнены все задания.
Шкала оценок по проценту правильно выполненных контрольных заданий	0 – 30 %	30 – 100 %

7.1. Описание шкал оценивания результатов обучения по дисциплине

Итоговый контроль качества усвоения студентами содержания дисциплины проводится в виде экзамена, на котором определяется:

- уровень усвоения студентами основного учебного материала по дисциплине;
- уровень понимания студентами изученного материала;
- способности студентов использовать полученные знания для решения конкретных задач.

Зачет проводится в устной форме и заключается в ответе студентом после предварительной подготовки на теоретические вопросы курса и решением практической задачи с последующим его обоснованием. По окончании ответа на вопросы билета в рамках тематики курса проводится собеседование в форме вопросов, на которые студент должен дать краткий ответ.

Зачтено	Отличная, хорошая или удовлетворительная подготовка. Обучаемый на удовлетворительно или лучше отвечает на вопросы программы–минимум и основной вопрос, а также на большинство дополнительных вопросов.
Не зачтено	Обучаемый показывает неудовлетворительное знание основ курса и базовых понятий, допускает значительные ошибки при ответах на большинство дополнительных вопросов. Необходима дополнительная подготовка для успешного прохождения испытания.

7.2. Критерии и процедуры оценивания результатов обучения по дисциплине (модулю), характеризующих сформированность компетенций

Для оценивания результатов обучения в виде знаний используются следующие процедуры и технологии:

- устные и письменные опросы.

Для оценивания результатов обучения в виде умений и владений используются следующие процедуры и технологии:

- практическое контрольное задание в виде проекта

Для проведения итогового контроля сформированности компетенции используются:

- письменные и устные ответы на теоретические вопросы,
- решение практических задач.

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих сформированность компетенций и (или) для итогового контроля сформированности компетенции.

Список вопросов по теории для оценки сформированности знаний компетенций:

УК-2

1. Математические основы криптографии
2. Основные понятия криптографии: шифр, алгоритм шифрования, ключ шифрования, криптосистема. Обобщенная схема для криптосистем с закрытыми ключами шифрования.
3. Основные исторические этапы становления криптографии. Криптографические и стеганографические методы защиты информации. Криптология, криптография и криптоанализ.
4. Основы криптоанализа. Определение. История создания частотного анализа. Попытки совершенствования одноалфавитного шифра.
5. Многоалфавитные шифры. Омофонический шифр замены. Диграф. Великий шифр. Шифр Билля.
6. Шифр Виженера. Беббидж и его роль во взломе шифра Виженера. Взлом шифра Виженера
7. Понятие вычета по модулю. Понятие сравнимости двух чисел.

8. Введение в конечные поля. Понятие группы. Циклическая группа. Правила выполнения операций в группах.
9. Кольцо. Кольцо с единицей. Подкольцо. Целостное кольцо. Поле. Порядок и степень поля. Поле Галуа. Прimitивный элемент конечного поля. Неприводимые многочлены. Умножение ненулевых элементов конечного поля.
10. Простые числа. Взаимно простые числа. Утверждение о сравнимости чисел. Понятие обратного числа. Утверждение о существовании обратного числа. Мультипликативность функции.
11. Теорема Ферма.
12. Функция Эйлера. Функция Мебиуса. Теорема Эйлера.
13. Алгоритм Евклида. Расширенный алгоритм Евклида.
14. Показатели и первообразные корни.
15. Генераторы случайных чисел. Методы построения ГСЧ. Проверка качества работы ГСЧ. Проверка на равномерность распределения. Проверка на статистическую независимость.
16. Преобразование Уолша-Адамара. Функции Уолша.
17. Эллиптические кривые. Безопасность систем дискретных логарифмов над эллиптическими кривыми.
18. Тесты числа на простоту. Принципы построения больших простых чисел. Алгоритм Адлемана-Ленстры. Разложение составных чисел на множители.
19. Дискретные логарифмы.
20. Понятие хеш-функции. Коллизия. Хеш-функции Наорра и Юнга. Проверка целостности информации с использованием хеш-функций. Построение хеш-функции на основе блочных преобразований. Нахождение коллизий хеш-функций в общем случае.
21. Парадокс о днях рождения. Атака «встреча посередине» для блочных хеш-функций.
22. Линейное разделение секрета.

Примеры проектов для зачета (для оценки сформированности знаний и умений компетенции ОПК-4)

- 6.1. нахождение чисел, относящихся к заданному показателю
- 6.2. Система открытого распределения ключей диффи хеллмана:
- 6.3. "Открытое шифрование Эль-Гамала" 10.1.1
- 6.4. Электронная цифровая подпись Эль-Гамала
- 6.5. Цифровая подпись Эль-Гамала с сокращенной длиной параметра s
- 6.6. вычисление мультипликативно обратных элементов в поле вычетов
- 6.7. Электронная цифровая подпись RSA
- 6.8. открытое распределение ключей с использованием криптосистемы RSA
- 6.9. Слепая подпись Шаума
- 6.10. Система открытого распределения ключей диффи хеллмана:
- 6.11. Цифровая подпись Эль-Гамала с сокращенной длиной параметра s

6.12. Методические материалы, определяющие процедуры оценивания.

Положение «О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в ННГУ», утвержденное приказом ректора ННГУ от 13.02.2014 г. №55-ОД,

Положение о фонде оценочных средств, утвержденное приказом ректора ННГУ от 10.06.2015 №247-ОД.

7. 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. Лапониная 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

8. Материально-техническое обеспечение дисциплины (модуля)

Для обучения студентов названной дисциплины имеются в наличии: специальные кабинеты, оборудованные мультимедийными средствами обучения; компьютерные классы, где имеется возможность выхода в Интернет; присутствует полный комплект лицензионного обеспечения, необходимый для работы компьютерных программ.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по специальности 02.04.02 «Фундаментальная информатика и информационные технологии».

Автор Лапинова С.А.

Рецензент Горбунов А.А.

Заведующий кафедрой Дубков А.А.

Программа одобрена на заседании методической комиссии
Радиофизического факультета от «25» мая 2023 года, протокол № 04/23.