Приложение 4

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

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

Рабочая программа дисциплины

Математические основы защиты информации и информационной безопасности

Уровень высшего образования
Магистратура

Направление подготовки / специальность
02.04.02 - Фундаментальная информатика и информационные технологии

Направленность образовательной программы
Биоинформатика

Форма обучения
очная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.01 Математические основы защиты информации и информационной безопасности относится к обязательной части 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**
УК-2: Способен управлять проектом на всех этапах его жизненного цикла	*УК-2.1: Знает структуру жизненного цикла проекта* *УК-2.2: Умеет адаптировать жизненный цикл под специфику конкретных проектов* *УК-2.3: Владеет методами управления проектом на всех этапах его жизненного цикла*	*УК-2.1: Способен сопровождать проект* *УК-2.2: Адаптирует цикл проекта под конкретную задачу* *УК-2.3: Применяет методы управления проектом*	*Собеседование*	*Зачёт: Проект*
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* *ОПК-4.2: Умеет осуществлять управление проектами информационных систем* *ОПК-4.3: Имеет практический опыт анализа и интерпретации информационных систем*	*ОПК-4.1: Применяет принципы сбора и анализа информации, создания информационных систем на стадиях жизненного цикла* *ОПК-4.2: осуществляет управление проектами информационных систем* *ОПК-4.3: Применяет практический опыт анализа и интерпретации информационных систем*	*Собеседование*	*Зачёт: Проект*

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная
Общая трудоемкость, з.е.	**3**
Часов по учебному плану	**108**
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	**32**
- занятия семинарского типа (практические занятия / лабораторные работы)	**0**
- КСР	**1**
самостоятельная работа	**75**
Промежуточная аттестация	**0** **Зачёт**

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	
	ооо	ооо	ооо	ооо	ооо
История развития криптографии. Основные понятия.	4	2		2	2
Математические основы криптографии.	12	4		4	8
Надежность шифров. Основы теории К. Шеннона	8	2		2	6
Хеш-функции	10	4		4	6
Введение в криптографические методы защиты информации	6	2		2	4
Системы симметричного шифрования	7	2		2	5
Системы асимметричного шифрования	10	4		4	6
Электронная цифровая подпись. Открытое распространение ключей	14	4		4	10
Криптографические методы защиты информации в телекоммуникационных сетях	12	2		2	10
Криптографические протоколы	10	2		2	8
Криптографические атаки	14	4		4	10
Аттестация	0				
КСР	1			1	
Итого	108	32	0	33	75

Содержание разделов и тем дисциплины

1. 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. Дикраф. 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.
10. Поле. Порядок и степень поля. Поле Галуа. Примитивный элемент конечного поля. Неприводимые многочлены. Умножение ненулевых элементов конечного поля.
11. Простые числа. Взаимно простые числа. Утверждение о сравнимости чисел. Понятие обратного числа. Утверждение о существовании обратного числа.
12. Мультипликативность функции.
13. Теорема Ферма.
14. Функция Эйлера. Функция Мебиуса. Теорема Эйлера.
15. Алгоритм Евклида. Расширенный алгоритм Евклида.
16. Показатели и первообразные корни.
17. Генераторы случайных чисел. Методы построения ГСЧ. Проверка качества работы ГСЧ. Проверка на равномерность распределения. Проверка на статистическую независимость.
18. Преобразование Уолша-Адамара. Функции Уолша.
19. Эллиптические кривые. Безопасность систем дискретных логарифмов над эллиптическими кривыми.
20. Тесты числа на простоту. Принципы построения больших простых чисел.
21. Алгоритм Адлемана-Ленстры. Разложение составных чисел на множители.
22. Дискретные логарифмы.
23. 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.
24. Парадокс о днях рождения. Атака «встреча посередине» для блочных хеш-функций.
25. Линейное разделение секрета.
26. Стойкость шифров. Правило Керкхоффа. Теоретическая и практическая стойкость криптосистем.
27. Теоретическая и практическая стойкость криптосистем. Теорема Шенона о совершенной секретности. Ненадежность шифров и расстояние единственности.
28. Понятие блочного и поточного шифра. Алгоритмы шифрования на основе сетей Фейстеля.
29. Стандарт шифрования данных DES. Основные характеристики. Обобщенная схема шифрования в алгоритме DES. Операции начальной и конечной перестановок. Схема вычисления функции шифрования для одного раунда алгоритма DES. Операции расширения и перестановки бит. Схема вычисления функции шифрования для одного раунда алгоритма DES. Операция преобразования на S-блоках. Схема вычисления раундовых ключей в алгоритме DES. Режимы работы блочных шифров. Комбинирование блочных шифров.
30. Стандарт шифрования ГОСТ 28147-89. Основные характеристики.
31. Стандарт шифрования AES. Основные характеристики.
32. Потоковые шифры A5 и RC4. Основные характеристики.
33. Криптография с открытыми ключами. Односторонние функции. Алгоритм Диффи-Хеллмана обмена ключевой информацией.

34. Криптосистема RSA.
35. Криптографические протоколы. Проблемы криптографических протоколов. Трехэтапный протокол Шамира.
36. Электронная цифровая подпись. Свойства электронной цифровой подписи.
37. Стандарт DSS. Схема генерации и проверки электронной цифровой подписи.
38. Криптографические функции хеширования. Основные требования, предъявляемые к криптографическим функциям хеширования. Алгоритм хеширования SHA.
39. Стандарты электронной цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и функции хеширования ГОСТ Р 34.11-94. Основные характеристики.
40. Открытое распространение ключей. Инфраструктура открытого распространения ключей и ее основные компоненты. Протоколы и механизмы аутентификации на основе открытых ключей и сертификатов (стандарт ITU-T X.509).
41. Системы электронной безопасности в финансовой сфере. Аутентификация данных на картах. Статическая и динамическая аутентификация.
42. Системы электронной безопасности в финансовой сфере. Системы аутентификации смарт-карт и терминалов на базе симметричных криптосистем

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.

https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=749494&idb=0

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 - Собеседование) для оценки сформированности компетенции УК-2:

1. 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. Дирграф. 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.

10. Поле. Порядок и степень поля. Поле Галуа. Примитивный элемент конечного поля. Неприводимые многочлены. Умножение ненулевых элементов конечного поля.
11. Простые числа. Взаимно простые числа. Утверждение о сравнимости чисел. Понятие обратного числа. Утверждение о существовании обратного числа.
12. Мультипликативность функции.
13. Теорема Ферма.
14. Функция Эйлера. Функция Мебиуса. Теорема Эйлера.
15. Алгоритм Евклида. Расширенный алгоритм Евклида.
16. Показатели и первообразные корни.
17. Генераторы случайных чисел. Методы построения ГСЧ. Проверка качества работы ГСЧ. Проверка на равномерность распределения. Проверка на статистическую независимость.
18. Преобразование Уолша-Адамара. Функции Уолша.
19. Эллиптические кривые. Безопасность систем дискретных логарифмов над эллиптическими кривыми.
20. Тесты числа на простоту. Принципы построения больших простых чисел.

5.1.2 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции ОПК-4:

1. Алгоритм Адлемана-Ленстры. Разложение составных чисел на множители.
2. Дискретные логарифмы.
3. 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.
4. Парадокс о днях рождения. Атака «встреча посередине» для блочных хеш-функций.
5. Линейное разделение секрета.
6. Стойкость шифров. Правило Керкхоффа. Теоретическая и практическая стойкость криптосистем.
7. Теоретическая и практическая стойкость криптосистем. Теорема Шенона о совершенной секретности. Ненадежность шифров и расстояние единственности.
8. Понятие блочного и поточного шифра. Алгоритмы шифрования на основе сетей Фейстеля.
9. Стандарт шифрования данных DES. Основные характеристики. Обобщенная схема шифрования в алгоритме DES. Операции начальной и конечной перестановок. Схема вычисления функции шифрования для одного раунда алгоритма DES. Операции расширения и перестановки бит. Схема вычисления функции шифрования для одного раунда алгоритма DES. Операция преобразования на S-блоках. Схема вычисления раундовых ключей в алгоритме DES. Режимы работы блочных шифров. Комбинирование блочных шифров.
10. Стандарт шифрования ГОСТ 28147-89. Основные характеристики.
11. Стандарт шифрования AES. Основные характеристики.
12. Потоковые шифры A5 и RC4. Основные характеристики.
13. Криптография с открытыми ключами. Односторонние функции. Алгоритм Диффи-Хеллмана обмена ключевой информацией.
14. Криптосистема RSA.
15. Криптографические протоколы. Проблемы криптографических протоколов. Трехэтапный протокол Шамира.
16. Электронная цифровая подпись. Свойства электронной цифровой подписи.
17. Стандарт DSS. Схема генерации и проверки электронной цифровой подписи.
18. Криптографические функции хеширования. Основные требования, предъявляемые к криптографическим функциям хеширования. Алгоритм хеширования SHA.
19. Стандарты электронной цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и функции хеширования ГОСТ Р 34.11-94. Основные характеристики.

20. Открытое распространение ключей. Инфраструктура открытого распространения ключей и ее основные компоненты. Протоколы и механизмы аутентификации на основе открытых ключей и сертификатов (стандарт ITU-T X.509).
21. Системы электронной безопасности в финансовой сфере. Аутентификация данных на картах. Статическая и динамическая аутентификация.

Критерии оценивания (оценочное средство - Собеседование)

Оценка	Критерии оценивания
зачтено	Все компетенции сформированы удовлетворительно
не зачтено	Хотя бы одна компетенция на уровне неудовлетворительно

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

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения 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 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.
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 несущественными недочетами, выполнены все	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

						задания в полном объеме	
Навыки	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 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 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 - Проект) для оценки сформированности компетенции УК-2

Написать код для шифрования методом DES

5.3.2 Типовые задания (оценочное средство - Проект) для оценки сформированности компетенции ОПК-4

1. Система открытого распределения ключей диффихеллмана:
2. "Открытое шифрование Эль-Гамаля" 10.1.1

3. Электронная цифровая подпись Эль-Гамаля
4. Цифровая подпись Эль-Гамаля с сокращенной длиной параметра s
5. вычисление мультипликативно обратных элементов в поле вычетов
6. Электронная цифровая подпись RSA
7. открытое распределение ключей с использованием криптосистемы RSA
8. Слепая подпись Шаума
9. Система открытого распределения ключей диффихеллмана:
10. Цифровая подпись Эль-Гамаля с сокращенной длиной параметра s

Критерии оценивания (оценочное средство - Проект)

Оценка	Критерии оценивания
зачтено	Знает основные понятия, способен объяснить структуру кода криптографической системы
не зачтено	Не знает основные понятия, не способен объяснить структуру кода криптографической системы

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

Основная литература:

1. Борисова С. Н. Криптографические методы защиты информации: классическая криптография : учебное пособие / Борисова С. Н. - Пенза : ПГУ, 2018. - 186 с. - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга из коллекции ПГУ - Информатика. - ISBN 978-5-907102-51-4., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=749494&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.

Дополнительная литература:

1. Запечников С. В. Криптографические методы защиты информации : учебник / С. В. Запечников, О. В. Казарин, А. А. Тарасов. - Москва : Юрайт, 2023. - 309 с. - (Высшее образование). - ISBN 978-5-534-02574-3. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=842677&idb=0.

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

Python 3.7. и выше

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/специальности 02.04.02 - Фундаментальная информатика и информационные технологии.

Автор(ы): Лапинова Светлана Александровна, кандидат физико-математических наук.

Заведующий кафедрой: Павлов Игорь Сергеевич, доктор физико-математических наук.

Программа одобрена на заседании методической комиссии от 18 декабря 2023, протокол № 09/23.