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

Алгоритмы идентификации динамических моделей криптосистем

Уровень высшего образования
Магистратура

Направление подготовки / специальность
02.04.02 - Фундаментальная информатика и информационные технологии

Направленность образовательной программы
Информационная безопасность и защита информации

Форма обучения
очная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.03 Алгоритмы идентификации динамических моделей криптосистем 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**
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:* *Знать:* *- основные подходы к построению математических моделей криптосистем и их функциональных элементов как динамических объектов* *- основные классы алгоритмов структурной и параметрической идентификации источников экспериментальных данных криптосистем* *УК-2.2:* *Уметь:* *- определять базовые параметры математических моделей криптосистем* *- оценивать параметры криптографической стойкости шифров на основе базовых параметров их экспериментальных данных* *- оценивать параметры вычислительной сложности алгоритмов идентификации динамических моделей криптосистем* *УК-2.3:* *Владеть:* *- методами идентификации моделей криптосистем по экспериментальным скалярным и векторным*	*Задания*	*Экзамен:* *Контрольные вопросы*

		данным *- навыками рационального выбора и реализации алгоритмов идентификации динамических моделей для типовых криптосистем*		
ПК-1: Способен руководить научными исследованиями и опытно-конструкторскими разработками, в области информатики и информационных технологий (ФИИТ), и формировать их новые направления в области профессиональной деятельности	*ПК-1.1: Знает проблематику и методы научных исследований и опытно-конструкторских разработок в области ФИИТ применительно к профессиональной деятельности* *ПК-1.2: Имеет навыки выполнения научных исследований и опытно-конструкторских разработок в области ФИИТ применительно к профессиональной деятельности* *ПК-1.3: Имеет навыки руководства исследованиями и опытно-конструкторскими разработками в области ФИИТ применительно к профессиональной деятельности, и формирования их новых направлений*	*ПК-1.1:* *Знать:* *- проблематику и методы научных исследований и опытно-конструкторских разработок в области идентификации динамических моделей криптосистем* *ПК-1.2:* *Уметь:* *- проводить научные исследования и опытно-конструкторские разработки в области идентификации динамических моделей криптосистем* *ПК-1.3:* *Владеть:* *- навыками руководства исследованиями и опытно-конструкторскими разработками в области идентификации динамических моделей криптосистем*	*Собеседование*	*Экзамен:* *Контрольные вопросы*

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная
Общая трудоемкость, з.е.	**4**
Часов по учебному плану	**144**
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	**32**
- занятия семинарского типа (практические занятия / лабораторные работы)	**0**
- КСР	**2**
самостоятельная работа	**65**
Промежуточная аттестация	**45**

	Экзамен

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	
	очно	очно	очно	очно	очно
1. Введение. Основные подходы к построению математических моделей криптосистем и их функциональных элементов как динамических объектов.	12	4		4	8
2. Алгоритмы структурной идентификации динамических моделей криптосистем.	45	16		16	29
3. Алгоритмы параметрической идентификации динамических моделей криптосистем.	40	12		12	28
Аттестация	45				
КСР	2			2	
Итого	144	32	0	34	65

Содержание разделов и тем дисциплины

1. Введение. Основные подходы к построению математических моделей криптосистем и их функциональных элементов как динамических объектов.
2. Алгоритмы структурной идентификации динамических моделей криптосистем.
3. Алгоритмы параметрической идентификации динамических моделей криптосистем.

Практические занятия /лабораторные работы организуются, в том числе, в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.
На проведение практических занятий / лабораторных работ в форме практической подготовки отводится: очная форма обучения - 4 ч.

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.

Электронно-библиотечная система "Юрайт".

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 - Задания) для оценки сформированности компетенции УК-2:

1. Программная реализация алгоритма нахождения базового параметра (БП) сложности автономного источника данных методом непосредственного перебора всех подпоследовательностей по выходной последовательности экспериментальных данных.
2. Программная реализация алгоритма нахождения БП сложности автономного источника данных методом бинарного поиска по выходной последовательности экспериментальных данных.
3. Программная реализация алгоритма нахождения БП сложности неавтономного преобразователя данных по входным и выходным последовательностям экспериментальных данных.
4. Программная реализация алгоритма параметрической идентификации моделей преобразователей текстовых последовательностей в алгебраических структурах модулярных полей.

Критерии оценивания (оценочное средство - Задания)

Оценка	Критерии оценивания
зачтено	Минимально допустимый уровень знаний и выше. Допущенные ошибки не являлись грубыми. Продемонстрированы основные умения, возможны негрубые ошибки. Имеется минимальный и выше набор навыков для решения стандартных заданий, допускаются некоторые недочеты.
не зачтено	Уровень знаний ниже минимальных требований. При решении стандартных заданий не продемонстрированы основные умения и базовые навыки. Имели место грубые ошибки.

5.1.2 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции ПК-1:

1. Сравнение оценок вычислительной сложности относительно длины обрабатываемой последовательности для основных классов алгоритмов структурной идентификации математических моделей источников экспериментальных данных:
- алгоритмы непосредственного вычисления базовых параметров
- алгоритмы бинарного поиска
- алгоритмы построения суффиксного дерева
2. Сравнение подходов к построению алгоритмов параметрической идентификации линейных и нелинейных математических моделей криптосистем по их экспериментальным данным.
3. Сравнение подходов к решению задач определения наборов базовых параметров и свободных параметров текстовых последовательностей криптосистем при различных размерностях их алфавитов.

Критерии оценивания (оценочное средство - Собеседование)

Оценка	Критерии оценивания
зачтено	Уровень знаний в полном объеме, соответствующем программе подготовки, допускаются несколько негрубых ошибок.
не зачтено	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.

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 задания в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие базовых навыков. Невозможность оценить наличие навыков	При решении стандартных задач не продемонстрированы базовые навыки. Имели	Имеется минимальный набор навыков для решения	Продемонстрированы базовые навыки при решении стандартны	Продемонстрированы базовые навыки при решении стандартны	Продемонстрированы навыки при решении нестандарт	Продемонстрирован творческий подход к решению нестандартны

	вследствие отказа обучающегося от ответа	место грубые ошибки	стандартны х задач с некоторым и недочетами	х задач с некоторым и недочетами	х задач без ошибок и недочетов	ных задач без ошибок и недочетов	х 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 - Контрольные вопросы) для оценки сформированности компетенции УК-2

1. Общая структурная схема криптосистемы. Динамическая математическая модель в форме синхронного автомата Хаффмана-Глушкова для основных функциональных элементов криптосистемы.
2. Задача структурной и параметрической идентификации математической модели криптосистемы как задача определения наборов базовых параметров и свободных параметров.
3. Текстовые последовательности криптосистемы как сигналы, порождаемые гипотетическими источниками экспериментальных данных. Глубина памяти и условие непротиворечивости таблицы истинности прогнозирующего оператора источника экспериментальных данных.
4. Векторные сигналы криптосистемы и объемы их фазовых пространств. Алгоритмическая реализация обработки векторных отсчетов текстовых сигналов.
5. Основные классы алгоритмов структурной идентификации математических моделей источников экспериментальных данных и оценки их вычислительной сложности относительно длины обрабатываемой последовательности данных.

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПК-1

1. Текстовые последовательности криптосистемы как сигналы, порождаемые гипотетическими источниками экспериментальных данных. Глубина памяти и условие непротиворечивости таблицы истинности прогнозирующего оператора источника экспериментальных данных.
2. Основные классы алгоритмов структурной идентификации математических моделей источников экспериментальных данных и оценки их вычислительной сложности относительно длины обрабатываемой последовательности данных.
3. Алгоритмы непосредственного вычисления базовых параметров. Вывод оценки времени работы алгоритмов относительно длины обрабатываемых тестовых последовательностей.
4. Алгоритмы определения базовых параметров на основе бинарного поиска. Вывод оценки времени работы алгоритмов относительно длины обрабатываемых тестовых последовательностей.
5. Алгоритмы определения базовых параметров на основе построения суффиксного дерева по обрабатываемой текстовой последовательности. Вывод оценки времени работы алгоритмов относительно длины обрабатываемых тестовых последовательностей.
6. Алгоритмы параметрической идентификации линейных математических моделей источников экспериментальных данных.
7. Подходы к построению алгоритмов параметрической идентификации нелинейных математических моделей криптосистем по экспериментальным данным.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
превосходно	Уровень знаний в объеме, превышающем программу подготовки. Продемонстрированы все основные умения. Выполнены все задания, в полном объеме без недочетов. Продемонстрирован творческий подход к решению нестандартных задач.
отлично	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок. Продемонстрированы все основные умения с отдельными несущественными недочетами, выполнены все задания в полном объеме. Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов.
очень хорошо	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок. Продемонстрированы все основные умения. Выполнены все задания, в полном объеме, но некоторые с недочетами. Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.
хорошо	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок. Продемонстрированы все основные умения с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами. Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами.
удовлетворительно	Минимально допустимый уровень знаний. Допущено много негрубых ошибки. Продемонстрированы основные умения с негрубыми ошибками.

Оценка	Критерии оценивания
	Выполнены все задания но не в полном объеме. Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами.
неудовлетворительно	Уровень знаний ниже минимальных требований. При решении стандартных задач не продемонстрированы основные умения и базовые навыки. Имели место грубые ошибки.
плохо	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа. Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа. Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа.

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

Основная литература:

1. Васильева И. Н. Криптографические методы защиты информации : учебник и практикум / И. Н. Васильева. - Москва : Юрайт, 2023. - 349 с. - (Высшее образование). - ISBN 978-5-534-02883-6. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=839932&idb=0.
2. Лось А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд. - Москва : Юрайт, 2023. - 473 с. - (Высшее образование). - ISBN 978-5-534-12474-3. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=840431&idb=0.
3. Кирьянов К. Г. Генетический код и тексты: динамические и информационные модели сложных систем / [ред. Л. Ю. Ротков, А. В. Якимов] ; ННГУ им. Н. И. Лобачевского. - Н. Новгород : Талам, 2002. - 100 с. - ISBN 5-93496-024-5 : 20.00., 2 экз.
4. Гроп Даниэль. Методы идентификации систем / пер. с англ. В. А. Васильева и В. И. Лопатина ; под ред. Е. И. Кринецкого. - М. : Мир, 1979. - 302 с. : ил. - 1.40., 1 экз.

Дополнительная литература:

1. Романец Юрий Васильевич. Защита информации в компьютерных системах и сетях / под ред. В. Ф. Шаньгина. - 2-е изд., перераб. и доп. - М. : Радио и связь, 2001. - 376 с. : ил. - ISBN 5-256-01518-4 : 78.00., 1 экз.
2. Современные методы идентификации систем / под ред. П. Эйкхоффа ; пер. с англ. под ред. Я. З. Цыпкина. - М. : Мир , 1983. - 400 с. : граф. - 2.60., 2 экз.

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

1. Национальный стандарт Российской Федерации ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры». – М.: Стандартинформ,

2015. (интернет-ресурс: http://protect.gost.ru/document1.aspx?control=7&id=200990 , интернет-ресурс: http://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf)
2. Национальный стандарт Российской Федерации ГОСТ Р 34.13–2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров». – М.: Стандартинформ, 2015. (интернет-ресурс: http://protect.gost.ru/document1.aspx?control=7&id=200971 , интернет-ресурс: http://www.tc26.ru/standard/gost/GOST_R_3413-2015.pdf)
3. ГОСТ Р 34.10–2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». – М.: Стандартинформ, 2013. (интернет-ресурс: http://protect.gost.ru/document.aspx?control=7&id=180151)
4. ГОСТ Р 34.11–2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». – М.: Стандартинформ, 2013. (интернет-ресурс: http://protect.gost.ru/v.aspx?control=7&id=180209)
5. Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_112701/)
6. ГОСТ Р 34.10–2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». – М.: Госстандарт России, 2001. (интернет-ресурс: http://protect.gost.ru/v.aspx?control=7&id=131131 , интернет-ресурс: http://standartgost.ru/g/ГОСТ_Р_34.10-2001)
7. FIPS Publication 197. Specification for the Advanced Encryption Standard (AES). – National Institute of Standards and Technology (NIST), 2001. (интернет-ресурс: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf)
8. FIPS Publication 46-3. Specifications for the Data Encryption Standard (DES). – National Institute of Standards and Technology (NIST), 1999. (интернет-ресурс: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)
9. ГОСТ Р 34.10–94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма». – М.: Госстандарт России, 1994. (интернет-ресурс: http://docs.cntd.ru/document/1200004855 , интернет-ресурс: http://standartgost.ru/g/ГОСТ_Р_34.10-94)
10. ГОСТ Р 34.11–94 «Информационная технология. Криптографическая защита информации. Функция хэширования». – М.: Госстандарт России, 1994. (интернет-ресурс: http://protect.gost.ru/document.aspx?control=7&id=134550 , интернет-ресурс: http://standartgost.ru/g/ГОСТ_Р_34.11-94)

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): Горбунов Александр Александрович.

Заведующий кафедрой: Ротков Леонид Юрьевич, кандидат технических наук.

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