

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

Специалитет

Направление подготовки / специальность

10.05.02 - Информационная безопасность телекоммуникационных систем

Направленность образовательной программы

Системы подвижной цифровой защищенной связи

Форма обучения

очная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.ДВ.06.02 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
ПК-2: Способен анализировать угрозы информационной безопасности цифровых телекоммуникационных сетей, контролировать их работоспособность и оценивать эффективность	<p>ПК-2.1: Знает: - методы создания моделей угроз информационной безопасности цифровых телекоммуникационных сетей - методики оценки уязвимостей цифровых телекоммуникационных сетей с точки зрения возможности НСД к ним</p> <p>ПК-2.2: Умеет: - проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты цифровых телекоммуникационных сетей - разрабатывать модели угроз, и систематизировать сведения об угрозах информационной безопасности</p> <p>ПК-2.3: Владеет: - навыками сбора и систематизации сведений об угрозах НСД к системам подвижной цифровой защищенной связи</p>	<p>ПК-2.1:</p> <p>Знать:</p> <ul style="list-style-type: none"> - основные подходы к построению математических моделей криптосистем и их функциональных элементов как динамических объектов - классы алгоритмов структурной и параметрической идентификации источников экспериментальных данных криптосистем - основные подходы к определению базовых и рабочих параметров моделей криптосистем в беспроводных системах связи <p>ПК-2.2:</p> <p>Уметь:</p> <ul style="list-style-type: none"> - 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 - оценивать параметры 	Задания	Зачёт: Контрольные вопросы

		<p>стойкости типовых систем криптографической защиты информации в системах подвижной цифровой защищенной связи</p> <p>ПК-2.3: Владеть: - методами идентификации моделей криптосистем по экспериментальным скалярным и векторным данным - навыками рационального выбора и реализации алгоритмов идентификации динамических моделей для типовых криптосистем в системах подвижной цифровой защищенной связи</p>		
--	--	---	--	--

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная
Общая трудоемкость, з.е.	2
Часов по учебному плану	72
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	32
- занятия семинарского типа (практические занятия / лабораторные работы)	0
- КСР	1
самостоятельная работа	39
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			Самостоятельная работа обучающегося, часы
		Контактная работа (работа во взаимодействии с преподавателем), часы из них			
		Занятия лекционного типа	Занятия семинарского типа (практические занятия/ лабора	Всего	

			торные работы), часы		
	о ф о	о ф о	о ф о	о ф о	о ф о
Введение. Основные подходы к построению математических моделей криптосистем и их функциональных элементов как динамических объектов.	14	4		4	10
Алгоритмы структурной идентификации динамических моделей криптосистем.	33	16		16	17
Алгоритмы параметрической идентификации динамических моделей криптосистем.	24	12		12	12
Аттестация	0				
КСР	1			1	
Итого	72	32	0	33	39

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 ПК-2:

1. Программная реализация алгоритма нахождения базового параметра (БП) сложности автономного источника данных методом непосредственного перебора всех n-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 автономного источника данных методом построения суффиксного дерева по выходной последовательности экспериментальных данных.

Критерии оценивания (оценочное средство - Задания)

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			
<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	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи с отдельными недочетами и, выполнены все	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

						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 - Контрольные вопросы) для оценки сформированности компетенции ПК-2

1. Задача структурной и параметрической идентификации математической модели криптосистемы как задача определения наборов базовых параметров и свободных параметров.
2. Основные классы алгоритмов структурной идентификации математических моделей источников экспериментальных данных и оценки их вычислительной сложности относительно длины обрабатываемой последовательности данных.

3. Алгоритмы определения базовых параметров на основе бинарного поиска. Вывод оценки времени работы алгоритмов относительно длины обрабатываемых тестовых последовательностей.

4. Алгоритмы параметрической идентификации линейных математических моделей источников экспериментальных данных.

Критерии оценивания (оценочное средство - Контрольные вопросы)

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.

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_P_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_P_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_P_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 ФГОС ВО по направлению подготовки/специальности 10.05.02 - Информационная безопасность телекоммуникационных систем.

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.