

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 ученого совета ННГУ

протокол от

«31» мая 2023 г. № 6

Рабочая программа дисциплины

Алгоритмы идентификации динамических
моделей криптосистем

(наименование дисциплины (модуля))

Уровень высшего образования

специалитет

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

10.05.02 Информационная безопасность телекоммуникационных систем

(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы

Системы подвижной цифровой защищенной связи

(указывается профиль / магистерская программа / специализация)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижегород

2023 год

1. Место дисциплины в структуре ООП

Дисциплина «Алгоритмы идентификации динамических моделей криптосистем» относится к части, формируемой участниками образовательных отношений, основной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

№ варианта	Место дисциплины в учебном плане образовательной программы	Стандартный текст для автоматического заполнения в конструкторе РПД
2	Блок 1. Дисциплины (модули) Часть, формируемая участниками образовательных отношений	Дисциплина Б1.В.ДВ.06.02 «Алгоритмы идентификации динамических моделей криптосистем» относится к части ООП специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», 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	
ПК-2. Способен анализировать угрозы информационной безопасности цифровых телекоммуникационных сетей, контролировать их работоспособность и оценивать эффективность	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	Знать: - 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	Собеседование
	ПК-2.2. Умеет: - проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты цифровых телекоммуникационных	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	Собеседование

	сетей - разрабатывать модели угроз, и систематизировать сведения об угрозах информационной безопасности	динамических моделей криптосистем - оценивать параметры стойкости типовых систем криптографической защиты информации в системах подвижной цифровой защищенной связи	
	ПК-2.3. Владеет: - навыками сбора и систематизации сведений об угрозах НСД к системам подвижной цифровой защищенной связи	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	Собеседование

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	2 ЗЕТ	___ ЗЕТ	___ ЗЕТ
Часов по учебному плану	72		
в том числе			
аудиторные занятия (контактная работа): - занятия лекционного типа - занятия семинарского типа (практические занятия / лабораторные работы)	32		
самостоятельная работа	39		
КСР	1		
Промежуточная аттестация – экзамен/зачет	зачет		

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины,	Всего (часы)	В том числе	
		Контактная работа (работа во взаимодействии с преподавателем), часы из них	рабо та обуч

форма промежуточной аттестации по дисциплине		Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Всего	
1. Введение. Основные подходы к построению математических моделей криптосистем и их функциональных элементов как динамических объектов.	14	4			4	10
2. Алгоритмы структурной идентификации динамических моделей криптосистем.	33	16			16	17
3. Алгоритмы параметрической идентификации динамических моделей криптосистем.	24	12			12	12
Итого:	71	32			32	39

Текущий контроль успеваемости реализуется в рамках занятий, лабораторного типа.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя изучение дополнительных разделов дисциплины с использованием учебной литературы.

Текущий контроль усвоения материала проводится путем проведения опроса.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

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

включающий:

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций	Шкала оценивания сформированности компетенций						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно

(индикатора достижения компетенций)							
<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, без ошибок.	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.	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
<u>Навыки</u>	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
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»
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

<i>Вопросы</i>	<i>Код формируемой компетенции</i>
1. Общая структурная схема криптосистемы. Динамическая математическая модель в форме синхронного автомата Хаффмана-Глушкова для основных функциональных элементов криптосистемы.	ПК-2
2. Задача структурной и параметрической идентификации математической модели криптосистемы как задача определения наборов базовых параметров и свободных параметров.	ПК-2
3. Текстовые последовательности криптосистемы как сигналы, порождаемые гипотетическими источниками экспериментальных данных. Глубина памяти и условие непротиворечивости таблицы истинности прогнозирующего оператора источника экспериментальных данных.	ПК-2
4. Векторные сигналы криптосистемы и объемы их фазовых пространств. Алгоритмическая реализация обработки векторных отсчетов текстовых сигналов.	ПК-2
5. Основные классы алгоритмов структурной идентификации математических моделей источников экспериментальных данных и оценки их вычислительной сложности относительно длины обрабатываемой последовательности данных.	ПК-2
6. Алгоритмы непосредственного вычисления базовых параметров. Вывод оценки времени работы алгоритмов относительно длины обрабатываемых тестовых последовательностей.	ПК-2
7. Алгоритмы определения базовых параметров на основе бинарного поиска. Вывод оценки времени работы алгоритмов относительно длины обрабатываемых тестовых последовательностей.	ПК-2
8. Алгоритмы определения базовых параметров на основе построения суффиксного дерева по обрабатываемой текстовой	ПК-2

последовательности. Вывод оценки времени работы алгоритмов относительно длины обрабатываемых тестовых последовательностей.	
9. Алгоритмы параметрической идентификации линейных математических моделей источников экспериментальных данных.	ПК-2
10. Подходы к построению алгоритмов параметрической идентификации нелинейных математических моделей криптосистем по экспериментальным данным.	ПК-2

5.2.2. Типовые задания для оценки сформированности компетенции ПК-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.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Васильева И.Н. Криптографические методы защиты информации. – М.: Издательство Юрайт, 2017. – 349 с. [Электронный ресурс: <https://biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2>]
2. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. – М.: Издательство Юрайт, 2017. – 473 с. [Электронный ресурс: <https://biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A>]
3. Кирьянов К.Г. Генетический код и тексты: динамические и информационные модели сложных систем. /Ред. Л.Ю. Ротков, А.В. Якимов. – Нижний Новгород: ТАЛАН, 2002. – 100 с.
4. Гроп Д. Методы идентификации систем. – М.: Мир, 1979. – 302 с.

б) дополнительная литература:

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.
2. Эйкхофф П. Современные методы идентификации систем. – М.: Мир, 1983. – 400 с.

в) 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

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и 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 специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Автор (ы) _____ А.А. Горбунов

Заведующий кафедрой «Безопасность информационных систем» _____ Л.Ю. Ротков

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