

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)

УТВЕРЖДАЮ:

Декан \_\_\_\_\_ Матросов В.В.

« 29 » \_\_\_\_\_ июня 2020 г.

**Рабочая программа дисциплины**

Б1.В.ДВ.07.02 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)

Квалификация (степень)

специалист

(бакалавр / магистр / специалист)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижний Новгород

2018

## 1. Место и цели дисциплины в структуре ОПОП

Дисциплина «Алгоритмы идентификации динамических моделей криптосистем» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», преподается в 10 семестре.

Изучение студентами дисциплины «Алгоритмы идентификации динамических моделей криптосистем» базируется на знаниях и умениях, полученных в результате изучения дисциплин «Теория автоматов и формальных языков», «Алгоритмы и анализ сложности», «Математические модели и идентификация», «Криптографические методы защиты информации».

### Целями освоения дисциплины являются:

Основной целью дисциплины «Алгоритмы идентификации динамических моделей криптосистем» является изложение принципов и методов нахождения математических моделей (идентификации) криптографических систем (криптосистем) на основе экспериментальных и/или априорных данных. Содержание дисциплины направлено на ознакомление студентов с использованием математических моделей и характеристик криптографических преобразователей информации, способов их структурной и параметрической идентификации.

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

Формируемые компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК-3. Способность оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств.  (этап освоения: завершающий)	31 (ПК-3). Знать основные подходы к построению математических моделей криптосистем и их функциональных элементов как динамических объектов. У1 (ПК-3). Уметь определять базовые параметры математических моделей криптосистем. У2 (ПК-3). Уметь оценивать параметры криптографической стойкости шифров на основе базовых параметров их экспериментальных данных. В1 (ПК-3). Владеть методами идентификации моделей криптосистем по экспериментальным скалярным и векторным данным.
ПК-4. Способность участвовать в разработке компонентов телекоммуникационных систем.  (этап освоения: завершающий)	31 (ПК-4). Знать основные классы алгоритмов структурной и параметрической идентификации источников экспериментальных данных криптосистем. У1 (ПК-4). Уметь оценивать параметры

	<p>вычислительной сложности алгоритмов идентификации динамических моделей криптосистем.</p> <p>В1 (ПК-4). Владеть навыками рационального выбора и реализации алгоритмов идентификации динамических моделей для типовых криптосистем.</p>
--	--

### 3. Структура и содержание дисциплины «Алгоритмы идентификации динамических моделей криптосистем»

Объем дисциплины составляет 3 зачетные единицы, всего 108 часов, из которых 34 часа составляет контактная работа обучающегося с преподавателем (32 часа занятия лекционного типа, в том числе 2 часа – мероприятия текущего контроля успеваемости, 2 часа – мероприятия промежуточной аттестации), 74 часа составляет самостоятельная работа обучающегося.

Наименование и краткое содержание разделов и тем дисциплины,  форма промежуточной аттестации по дисциплине	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	Занятия лабораторного типа	Всего	
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.	52	16			16	36
3. Алгоритмы параметрической идентификации динамических моделей криптосистем.	42	12			12	30
В т.ч. текущий контроль	2	2			2	

#### 4. Образовательные технологии

Образовательные технологии, способствующие формированию компетенций, используемые на занятиях лекционного типа:

- лекции с изложением учебного материала.

#### 5. 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.

#### 6. Фонд оценочных средств для промежуточной аттестации по дисциплине, 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.

Индикаторы компетенции	Критерии оценивания						
	«плохо»	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«очень хорошо»	«отлично»	«превосходно»
<u>Знания</u>	Отсутствие знаний материала	Наличие грубых ошибок в основном материале	Знание основного материала с рядом негрубых ошибок	Знание основного материала с рядом заметных погрешностей	Знание основного материала с незначительными и погрешностями	Знание основного материала без ошибок и погрешностей	Знание основного и дополнительного материала без ошибок и погрешностей
<u>Умения</u>	Отсутствие способности решения стандартных задач	Наличие грубых ошибок при решении стандартных задач	Способность решения основных стандартных задач с существенными ошибками	Способность решения всех стандартных задач с незначительными погрешностями	Способность решения всех стандартных задач без ошибок и	Способность решения стандартных и некоторых нестандартных задач	Способность решения стандартных задач и широкого круга нестандартных

					погрешностей		артных задач
<u>Навыки</u>	Полное отсутствие навыка	Отсутствие навыка	Владение навыком в минимальном объеме	Посредственное владение навыком	Достаточное владение навыком	Хорошее владение навыком	Всестороннее владение навыком

## 6.2. Описание шкал оценивания.

Контроль качества усвоения студентами содержания дисциплины проводится в виде экзамена.

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

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.

## Критерии оценок.

Оценка	Уровень подготовки
Превосходно	Высокий уровень подготовки, безупречное владение теоретическим материалом, студент демонстрирует творческий подход к решению нестандартных ситуаций. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждая теоретический материал практическими примерами.
Отлично	Высокий уровень подготовки с незначительными ошибками. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждает теоретический материал практическими примерами.
Очень хорошо	Хорошая подготовка. Студент дает ответ на все теоретические вопросы билета при наличии неточностей.
Хорошо	В целом хорошая подготовка с заметными ошибками или недочетами. Студент дает полный ответ на все теоретические вопросы билета при наличии неточностей. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы экзаменатора.
Удовлетворительно	Минимально достаточный уровень подготовки. Студент показывает минимальный уровень теоретических знаний, делает существенные ошибки, но при ответах на наводящие вопросы, может правильно сориентироваться и в общих чертах дать правильный ответ.
Неудовлетворительно	Подготовка недостаточная и требует дополнительного изучения материала. Студент дает ошибочные ответы, как на теоретические вопросы билета, так и на дополнительные вопросы экзаменатора.
Плохо	Подготовка абсолютно недостаточная. Студент не отвечает на поставленные вопросы.

### **6.3. Критерии и процедуры оценивания результатов обучения по дисциплине, характеризующих этапы формирования компетенций.**

Для оценивания результатов обучения в виде **знаний** используются следующие процедуры и технологии: экзамен, проводимый в письменной форме с дальнейшим индивидуальным собеседованием.

Для оценивания результатов обучения в виде **умений** и **навыков** используются результаты обсуждения типовых криптографических решений в контексте их использования в реальных ситуациях.

### **6.4. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций и (или) для итогового контроля сформированности компетенции.**

#### **Типовые задания (оценочные средства), выносимые на экзамен.**

##### **6.4.1. Задания для оценки компетенции «ПК-3»:**

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.

##### **6.4.2. Задания для оценки компетенции «ПК-4»:**

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.

#### **6.5. 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 г. №247-ОД.

### **7. 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:**

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](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](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/](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](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](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](http://standartgost.ru/g/ГОСТ_P_34.11-94))

## **8. Материально-техническое обеспечение дисциплины**

Аудиторный фонд ННГУ для проведения лекций.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ОПОП ВПО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Автор (ы) \_\_\_\_\_ Л.Ю. Ротков

\_\_\_\_\_ А.А. Горбунов

Рецензент (ы) \_\_\_\_\_ С.Н. Жуков

Заведующий кафедрой «Безопасность  
информационных систем» \_\_\_\_\_ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от «25» июня 2020 года, протокол № 03/20.