



Основная профессиональная образовательная программа
01.04.01 Математика
(Фундаментальная математика)

Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра прикладной математики и компьютерных наук

ОДОБРЕНО:

Руководитель ОП

 Д. Н. Азаров
(подпись)

« 13 » июня 2018 г.

Рабочая программа дисциплины

Дополнительные главы компьютерной математики

Уровень высшего образования:	магистратура
Квалификация выпускника:	магистр
Направление подготовки:	01.04.01 Математика
Направленность (профиль) образовательной программы:	Фундаментальная математика
Тип образовательной программы:	программа академической магистратуры

Иваново



1. Цели освоения дисциплины

Цель курса состоит в знакомстве студентов с основными принципами построения блочных и поточных шифров, основами криптоанализа.

2. Место дисциплины в структуре ОП

Дисциплина входит в вариативную часть ОП. Для ее успешного изучения необходимы знания и умения, приобретенные в результате изучения следующих дисциплин: дополнительные главы алгебры; дополнительные главы математического анализа и геометрии. Данная дисциплина должна подготовить студентов к освоению следующих дисциплин и практик: специальные разделы компьютерной математики; избранные вопросы компьютерной математики; научно-производственная практика; преддипломная практика.

Для освоения данной дисциплины обучающийся должен:

Знать: основные понятия алгебры и математического анализа, принципы функционирования ЭВМ.

Уметь: производить вычисления в кольцах вычетов и многочленов.

Владеть: навыками алгоритмизации и программирования.

3. Планируемые результаты обучения по дисциплине

3.1. Компетенции, формированию которых способствует дисциплина

При освоении дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

а) общекультурные (ОК):

ОК-1 Способность к абстрактному мышлению, анализу, синтезу

б) общепрофессиональные (ОПК):

ОПК-1 Способность находить, формулировать и решать актуальные и значимые проблемы фундаментальной и прикладной математики

ОПК-2 Способность создавать и исследовать новые математические модели в естественных науках

в) профессиональные (ПК):

ПК-1 Способность к интенсивной научно-исследовательской работе

г) дополнительные (ПКВ):

ПКВ-1 Способность использовать знания математики и компьютерных наук в различных сферах профессиональной деятельности, в том числе в образовании, в областях, использующих математические методы и компьютерные технологии

3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с формируемыми компетенциями

В результате освоения дисциплины обучающийся должен:

Знать:

– основные результаты о блочных и поточных шифрах, их смысл, математическое выражение и способы применения в конкретной ситуации, а также методику математического аппарата, применяемого в данной области, и способы интерпретации полученного математического результата в терминах данной области (ОПК-2)

Уметь:

– строить математические модели шифрсистем (ОПК-2)

– с использованием методов абстрактного мышления, анализа и синтеза анализировать альтернативные варианты решения исследовательских задач в области криптографии и оценивать эффективность реализации этих вариантов (ОК-1, ПКВ-1)



Основная профессиональная образовательная программа
01.04.01 Математика
(Фундаментальная математика)

Владеть:

- современными математическими и компьютерными методами оценки шифров (ОПК-1, ПКВ-1)
- навыками решения исследовательских и практических задач в области криптографии (ОПК-1, ПК-1)

4. Объем и содержание дисциплины

Объем дисциплины составляет 3 зачетные единицы (108 академических часов).

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

Объем иной контактной работы и самостоятельной работы обучающегося по дисциплине указан в учебном плане образовательной программы.

№ п/п	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в ак. часах, по очной форме обучения)		Формы текущего контроля успеваемости (по очной форме обучения) Формы промежуточной аттестации
			Занятия лекционного типа	Занятия семинарского типа	
1.	Основы криптографии	1	4	4	
2.	Основы криптоанализа	1	4	2	
3.	Блочные шифры	1	4	4	
4.	Поточные шифры	1	4	4	
Итого за семестр:			16	14	Зачет
Итого по дисциплине:			16	14	Зачет

4.2. Развернутое описание содержания дисциплины по разделам (темам)

1. Основы криптографии

- 1.1. Формальное определение шифра
- 1.2. Шифры перестановки
- 1.3. Поточные шифры простой замены
- 1.4. Блочные шифры простой замены
- 1.5. Многоалфавитные шифры замены
- 1.6. Дисковые многоалфавитные шифры замены
- 1.7. Шифры гаммирования
2. Основы криптоанализа
 - 2.1. Характеристики текстовых сообщений
 - 2.2. Криптоанализ шифров перестановки
 - 2.3. Криптоанализ шифров простой замены
 - 2.4. Криптоанализ шифра гаммирования с периодической гаммой
 - 2.5. Криптоанализ шифра гаммирования с непериодической гаммой
3. Блочные шифры
 - 3.1. Принципы построения блочных шифров
 - 3.2. Алгоритм DES
 - 3.3. Алгоритм «Магма» (ГОСТ 28147-89)
 - 3.4. Алгоритм AES
 - 3.5. Алгоритм «Кузнечик» (ГОСТ Р 34.12-2015)
 - 3.6. Режимы использования блочных шифров
 - 3.7. Элементы криптоанализа блочных шифров



Основная профессиональная образовательная программа
01.04.01 Математика
(Фундаментальная математика)

4. Поточные шифры

- 4.1. Свойства и принципы построения поточных шифров
- 4.2. Линейные регистры сдвига
- 4.3. Усложнение генераторов ЛРП
- 4.4. Примеры поточных шифров

5. Образовательные технологии

Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине: технология проблемного обучения

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: технологии смешанного обучения.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Студенты выполняют самостоятельный поиск дополнительной информации по темам, перечисленным в п. 4.1, используя литературу, электронные ресурсы и базы данных, перечисленные в п. 8.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Промежуточная аттестация по дисциплине проводится в форме собеседования. Перечень вопросов к собеседованию содержится в приложении 2.

Оценка «зачтено» выставляется студенту, если он

Знает основные результаты о блочных и поточных шифрах, их смысл, математическое выражение и способы применения в конкретной ситуации, а также методику математического аппарата, применяемого в данной области, и способы интерпретации полученного математического результата в терминах данной области.

Умеет строить математические модели шифрсистем.

Владеет современными математическими и компьютерными методами оценки шифров.

Умеет с использованием методов абстрактного мышления, анализа и синтеза анализировать альтернативные варианты решения исследовательских задач в области криптографии и оценивать эффективность реализации этих вариантов.

Владеет навыками решения исследовательских и практических задач в области криптографии.

Итоговая оценка по дисциплине совпадает с оценкой, полученной на зачете.

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Креопалов, В.В. Технические средства и методы защиты информации. Учебн : практическое пособие [Электронный ресурс] / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. - URL: <http://biblioclub.ru/index.php?page=book&id=90753>

2. Анализ состояния защиты данных в информационных системах. Учебно-методическое пособие [Электронный ресурс] / Новосибирск : НГТУ, 2012. - 52 с. - URL: <http://biblioclub.ru/index.php?page=book&id=228844>

Дополнительная литература:

1. Титов, А.А. Технические средства защиты информации : учебное пособие / А.А. Титов. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 194 с. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=208661>



Основная профессиональная образовательная программа
01.04.01 Математика
(Фундаментальная математика)

2.Сергеева, Ю.С. Защита информации: Конспект лекций : учебное пособие / Ю.С. Сергеева. - М. : А-Приор, 2011. - 128 с. - (Конспект лекций). - ISBN 978-5-384-00397-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=72670>

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Система электронной поддержки образовательного процесса «Мой университет»
<https://uni.ivanovo.ac.ru>

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» www.biblioclub.ru

Электронная библиотека ИвГУ <http://lib.ivanovo.ac.ru>

Электронный каталог НБ ИвГУ <http://lib.ivanovo.ac.ru/index.php/ek>

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения;

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: демонстрационные устройства; электронные пособия презентации



Основная профессиональная образовательная программа
01.04.01 Математика
(Фундаментальная математика)

Автор(ы) рабочей программы дисциплины: зав. кафедрой ПМиКН, доцент, канд. физ.-мат. наук Соколов Е. В.

Программа рассмотрена и утверждена на заседании кафедры прикладной математики и компьютерных наук

«01» июня 20 18 г., протокол № 9

Программа обновлена

протокол заседания кафедры № 1 от «30» августа 2019 г.

Согласовано:

Руководитель ОП  Д.Н. Азаров
(подпись)

Программа обновлена

протокол заседания кафедры № _____ от «_____» _____ 20__ г.

Согласовано:

Руководитель ОП _____
(подпись)

Программа обновлена

протокол заседания кафедры № _____ от «_____» _____ 20__ г.

Согласовано:

Руководитель ОП _____
(подпись)