БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе
и образовательным инновациям

_____ О.И.Чуприс
(подпись) (И.О.Фамилия)

18.06.2018
(дата утверждения)

Регистрационный № УД-5492/уч.

СОВРЕМЕННЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

Учебная программа учреждения высшего образования по учебной дисциплине для специальности второй ступени высшего образования (магистратура) с углубленной подготовкой специалиста:

1-31 81 06 Веб-программирование и интернет-технологии
1-31 81 07 Математическое и программное обеспечение мобильных устройств

2018 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-31 81 07-2013 и учебных планов № G31-227/уч., № G31-228/уч. от 10.04.2017 г., № G31з-230/уч., № G31з-231/уч. От 26.05.2017.

СОСТАВИТЕЛИ:

Борис Михайлович ДУБРОВ, доцент кафедры Веб-технологий и компьютерного моделирования, кандидат физико-математических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой веб-технологий и компьютерного моделирования
(протокол № 8 от 13.06.2018г.);

Научно-методическим советом Белорусского государственного университета
(протокол № 6 от 16.06.2018г.).

Зав. каф.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Целью дисциплины является изучение наиболее востребованных математических моделей в современных компьютерных технологиях. Это включает в себя математические модели компиляторов и теорию формальных языков на основе идемпотентного анализа, методы эллиптической криптографии на основе теории чисел, математические модели обработки изображений на основе дискретного преобразования Фурье, использование криптографических алгоритмов в технологиях распределенных хранилищ данных.

Эти и другие математические модели являются сегодня базовыми строительными блоками современных компьютерных технологий и активно используются как при разработке программного обеспечения, так и для других прикладных задач, включая защиту информации, моделирование сложных процессов, анализ данных и ряд задач компьютерной графики.

Дисциплина «Современные проблемы математики компьютерных наук» покрывает важный раздел компьютерного моделирования и необходим как пользователям современных компьютерных систем, так и разработчикам программного обеспечения.

Учебная программа дисциплины «Современные проблемы математики компьютерных наук» разработана для магистрантов 1-го года обучения (1-й семестр) очной и заочной форм обучения по специальностям 1-31 81 06 Веб-программирование и интернет-технологии, 1-31 81 07 Математическое и программное обеспечение мобильных устройств механико-математического факультета Белорусского государственного университета.

Программа дисциплины «Современные проблемы математики компьютерных наук» составлена с учетов межпредметных связей и программ по смежным дисциплинам:

- .NET технологии
- Технологии Java EE

Целью дисциплины «Современные проблемы математики компьютерных наук» является необходимость обучения студентов навыкам анализа и проектирования программных продуктов, характеризующихся наличием наукоемких технологий.

Задачи дисциплины состоят в том, чтобы ознакомить студентов с методами применения базовых знаний по математическим дисциплинам к технологиям проектирования архитектуры компьютерных приложений.

В результате изучения дисциплины студент должен

знать:

- модель теории формальных языков на основе идемпотентного анализа;
- модели ассиметричной криптографии на основе теории чисел и эллиптических кривых;
- модель дискретного преобразования Фурье на основе теории конечных абелевых групп;
- модель распределенного хранилища данных и роль криптографических алгоритмов в блокчейн технологиях;

уметь:

- распознавать известные математические модели в задачах по разработке программного обеспечения;

владеть:

- навыками формализации задачи в области информационных технологий на математическом языке;
- навыками проектирования архитектуры информационных систем на основе теории конечных автоматов;
- техникой программирования алгоритмов криптографии, построения линейных фильтров на основе дискретного преобразования Фурье, построения распределенных хранилищ данных на основе блокчейн.

Преподавание данной дисциплины должно строиться таким образом, чтобы обучающийся приобретал следующие академические профессиональные компетенции:

- АК-1. Осуществлять самостоятельную научно-исследовательскую деятельность.
- АК-3. Использовать междисциплинарный подход при решении проблем.
- АК-4. Применять технические устройства и компьютеры, использовать базы данных, пакеты прикладных программ и средства компьютерной графики для решения профессиональных задач.
- АК-5. Постоянно повышать свою квалификацию.
- ПК-2. Разрабатывать и использовать современное учебно-методическое обеспечение.
- ПК-3. Осваивать и внедрять в учебный процесс инновационные образовательные технологии.
- ПК-7. Квалифицированно проводить научные исследования в области математики и информационных технологий.
- ПК-8. Пользоваться глобальными информационными ресурсами.
- ПК-11. Взаимодействовать со специалистами смежных профилей.

Также подлежат развитию социально-личностные компетенции магистра, его способности:

- СЛК-1. К сотрудничеству и работе в команде.
- СЛК-2. Владению коммуникативными способностями для работы в междисциплинарной и международной среде.
- СЛК-3. Совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования совей личности.
- СЛК-6. Проявлять инициативу и креативность, в том числе в нестандартных ситуациях.
- СЛК-7. Адаптироваться к новым ситуациям социально-профессиональной деятельности, реализовывать накопленный опыт, свои возможности.

Дисциплина «Современные проблемы математики компьютерных наук» относится к циклу дисциплин специальной подготовки (государственный компонент).

В соответствии с учебными планами специальностей на изучение дисциплины отводится.

Форма обучения	Срок обучения, лет	Дисциплина	Семестр	Экзамен семестр	Зачет семестр	Всего часов	В том числе ауд.	Из них	
								лекций	лабораторных
дневная	2	1	1		1	96	32	32	
заочная	2,5	1	1		1	96	10	10	

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

1. Введение

Роль фундаментальных математических исследований в развитии компьютерных технологий. Обзор наиболее востребованных математических моделей в современных компьютерных технологиях.

2. Теория формальных языков и идемпотентный анализ

Понятия идемпотентного анализа. Формальные языки, основные операции, структура идемпотентного полукольца. Определение регулярного языка и связь с регулярными выражениями. Понятие формальной грамматики. Примеры и классификация грамматик по Хомскому. Регулярные грамматики. Построение регулярного выражения по регулярной грамматике как решение системы линейных уравнений. Детерминированные и недетерминированные конечные автоматы. Использование языка идемпотентного анализа для решения задач оптимизации на графах.

3. Математические модели криптографии

Элементы теории чисел в терминах теории колец и полей. Математическая модель ассиметричного кодирования. Геометрия эллиптических кривых над полем комплексных чисел. Введение в теорию конечных полей. Криптография с использованием эллиптических кривых над конечными полями

4. Функциональный анализ и сжатие изображений

Характеры конечных групп. Дискретное преобразование Фурье как теория характеров конечных циклических групп. Особенности компьютерной реализации и методы параллелизации. Дискретное преобразование косинусов в формате JPEG. Понятие вейвлетов. Примеры построения вейвлетов. Математическая модель формата JPEG2000.

5. Распределенные хранилища данных на основе блокчейн

Общие принципы построения распределенных СУБД. Блоки трансакций и защищенные цепочки блоков. Древовидное хеширование. Протоколы цифровой подписи, основанные на асимметричном шифровании. Принципы подтверждения трансакций и оценка сложности вычислений. Примеры практический применений.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
(очная форма обучения)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1	**Теория формальных языков**	**10**						
1.1	Понятие формального языка. Основные операции и их свойства. Синтаксис регулярных выражений. Определение регулярного языка.	2						
1.2	Лемма о разрастании. Примеры нерегулярных языков. Понятие конечного автомата. Задание формальных языков при помощи конечных автоматов. Синтез конечных автоматов по регулярных выражениям.	2						
1.3	Введение в идемпотентную математику. Приложения к задачам оптимизации на графах.	2						
1.4	Практикум по задачам формальной теории языков и идемпотентной математике	2						Опрос
1.5	Текущий контроль знаний (контрольная работа)	2						**Контрольная работа 1**
2	**Дискретное преобразование Фурье и методы обработки изображений**	**10**						
2.1	Определение дискретного преобразования Фурье. Интерпретация на языке линейной алгебры. Основные свойства дискретного пре-	2						

	образования Фурье.							
2.2	Обратное дискретное преобразование Фурье. Случай составной длины сигнала	2						
2.3	Быстрое преобразование Фурье: принципы и основные шаг, оценка сложности	**2**						
2.4	Быстрое преобразование Фурье: формальный алгоритм, примеры для n=4,8	2						Опрос
2.5	Текущий контроль знаний (контрольная работа)	2						**Контроль-ная работа 2**
3	**Математические модели криптографии и технологии блокчейн**	**12**						
3.1	Краткий обзор математических моделей в теории чисел и крипто-графии	2						
3.2	Принципы ассиметричной криптографии. Интерпретация алгоритма RSA в терминах конечных абелевых групп.	2						
3.3	Введение в теорию эллиптических кривых над конечными полями. Структура абелевой группы на множестве точек эллиптической кривой. Протоколы эллиптической криптографии.	2						
3.4	Общие принципы построения распределенных СУБД. Блоки тран-сакций и защищенные цепочки блоков. Древовидное хеширование.	2						
3.5	Протоколы цифровой подписи, основанные на асимметричном шифровании. Принципы подтверждения трансакций и оценка сложности вычислений. Примеры практический применений.	2						
3.6	Текущий контроль знаний (контрольная работа)	2						**Контроль-ная работа 3**
ВСЕГО		**32**						
								Зачет

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
(заочная форма обучения)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1	**Теория формальных языков**	**3**						
1.1	Понятие формального языка. Основные операции и их свойства. Синтаксис регулярных выражений. Определение регулярного языка.	1						
1.2	Лемма о разрастании. Примеры нерегулярных языков. Понятие конечного автомата. Задание формальных языков при помощи конечных автоматов. Синтез конечных автоматов по регулярных выражениям.	1						
1.3	Введение в идемпотентную математику. Приложения к задачам оптимизации на графах.	1						**Контрольная работа 1**
2	**Дискретное преобразование Фурье и методы обработки изображений**	**3**						
2.1	Определение дискретного преобразования Фурье. Интерпретация на языке линейной алгебры. Основные свойства дискретного преобразования Фурье.	1						
2.2	Обратное дискретное преобразование Фурье. Случай составной длины сигнала	1						
2.3	Быстрое преобразование Фурье: принципы и основные шаг, оценка	1						Опрос

	сложности, формальный алгоритм, примеры для n=4,8.							
3	**Математические модели криптографии и технологии блокчейн**	**4**						
3.1	Краткий обзор математических моделей в теории чисел и криптографии. Принципы ассиметричной криптографии. Интерпретация алгоритма RSA в терминах конечных абелевых групп.	1						
3.2	Введение в теорию эллиптических кривых над конечными полями. Структура абелевой группы на множестве точек эллиптической кривой. Протоколы эллиптической криптографии.	1						
3.4	Общие принципы построения распределенных СУБД. Блоки транзакций и защищенные цепочки блоков. Древовидное хеширование.	1						
3.5	Протоколы цифровой подписи, основанные на асимметричном шифровании. Принципы подтверждения трансакций и оценка сложности вычислений. Примеры практический применений.	1						**Контрольная работа 2**
ВСЕГО		**10**						
								Зачет

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ
ЛИТЕРАТУРА

Основная литература

1. А. Ахо, Дж. Ульман, Р. Сети. Компиляторы: принципы, технологии и инструменты. – СПб: Вильямс, 2001.
2. Ю.С. Харин, В.И. Берник, Г.В. Матвеев. Математические и компьютерные основы криптологии. Минск: Новое знание, 2003.
3. Э. Столниц, Т. ДеРоуз, Д. Салезин. Вейвлеты в компьютерной графике. Теория и приложения. М.: Регулярная и хаотическая динамика. 2002.
4. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto Institute. October 31, 2008.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Индивидуальные задания повышенной сложности для управляемой самостоятельной работы включают решение задач, выходящих за рамки основной программы дисциплины, которые сдаются на проверку в письменном виде.

Раздел 1. Теория формальных языков и идемпотентная математика

1. Привести примеры нерегулярных языков, которые могут быть распознаны при помощи бесконечных автоматов.
2. Привести примеры (с доказательством) языков, которые не могут быть описаны при помощи контекстно-свободной грамматики.
3. Переформулировать классические алгоритмы дискретной оптимизации на языке идемпотентной математики.
4. Реализовать алгоритм поиска оптимального пути на графе через перегрузку операций сложения и умножения.

Раздел 2. Математические модели криптографии

1. Реализовать PKS алгоритм ассиметричной криптографии.

Раздел 3. Дискретное преобразование Фурье

1. Спроектировать схему быстрого преобразования Фурье с 16, 32 входными сигналами.
2. Реализовать алгоритм сглаживания изображений на основе быстрого преобразования Фурье.

Раздел 4. Блокчейн технологии

1. Построить прототип распределенного хранилища данных с узлами сети, расположенными на компьютерах учащихся.

СРЕДСТВА ДИАГНОСТИКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

Рекомендуются следующие формы диагностики компетенций.

Устная форма

1. Опрос.

Письменная форма

1. Контрольные работы.

Устно-письменная форма

1. Зачет

ПРОТОКОЛ
СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
.NET технологии	Веб-технологий и компьютерного моделирования	Нет	Вносить изменения не требуется (протокол №8 от 13.06.2018г.)
Технологии Java EE	Веб-технологий и компьютерного моделирования	Нет	Вносить изменения не требуется (протокол №8 от 13.06.2018г.)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры *Веб–технологий и компьютерного моделирования* (протокол № ___ от _____ 201_ г.)

Заведующий кафедрой

канд. физ.-мат. наук, доцент _____ В.С. Романчик
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

канд. физ.-мат. наук, доцент _____ Д.Г. Медведев
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)