**ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»**

**ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

Кафедра теории упругости и вычислительной математики
имени академика А.С. Космодамианского

**УТВЕРЖДАЮ:**
проректор по научно-методической
и учебной работе
_____ Е.И. Скафа
«22» апреля 2020 г.
МП

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ»

| | |
|---|---|
| Направление подготовки: | 01.04.02 Прикладная математика и информатика |
| Магистерская программа: | Прикладная математика и информатика |
| Образовательная программа: | академическая магистратура |
| Квалификация: | Магистр |
| Форма обучения: | очная, очно-заочная, заочная<br>нужное подчеркнуть |

Донецк 2020

**УТВЕРЖДАЮ:**
Декан факультета математики
и информационных технологий
_____ И. А. Моисеенко
«16» апреля 2020 г.
МП

Программа составлена на основании Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) направления подготовки 01.04.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки Российской Федерации от ««12» марта 2015 г. № 228;
Порядка организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики, утвержденного приказом Министерства образования и науки ДНР № 1171 от «10» ноября 2017 г.;
учебного плана и основной образовательной программы Прикладная математика и информатика, направления подготовки 01.04.02 Прикладная математика и информатика, разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:
Доцент кафедры теории упругости и
вычислительной математики имени
академика А.С. Космодамианского _____ В.Н. Неспирный

Программа учебной дисциплины утверждена на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского

Протокол № 11 от «9» апреля 2020 г.
Заведующий кафедрой _____ В.И. Сторожев

Программа учебной дисциплины одобрена учебно-методической комиссией факультета математики и информационных технологий
Протокол № 8 от «15» апреля 2020 г.

Председатель учебно-методической
комиссии факультета _____ Л.И. Селякова

## 1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Современные проблемы прикладной математики и информатики» относится к базовой части учебного плана и состоит из одного модуля.

В рамках данной дисциплины изучаются современные проблемы, связанные с созданием и функционированием криптовалют и технологии блокчейн, рассматриваются экономические и технологические основы этих технологий и возможные сферы их применения.

Для изучения учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими и сопутствующими дисциплинами учебного плана подготовки бакалавров по направлению 01.03.02 Прикладная математика и информатика:

Основы программирования

Теория вероятностей и математическая статистика

Математические основы защиты информации

Частично используются, но не являются критически необходимыми для успешного освоения данного курса понятия и знания, полученные студентами при изучении следующих дисциплин:

Теория алгоритмов

Алгоритмы и структуры данных

Базы данных и информационные системы

Компьютерные сети

Современные методы криптографии

## 2. СТРУКТУРА ДИСЦИПЛИНЫ

| ***Характеристика учебной дисциплины*** | | |
|---|---|---|
| Направление подготовки | 01.04.02 Прикладная математика и информатика | |
| Магистерская программа | Прикладная математика и информатика | |
| Образовательная программа | академическая магистратура | |
| Квалификация | магистр | |
| Количество содержательных модулей | 3 | |
| Дисциплина базовой / вариативной части образовательной программы | Базовая часть профессионального блока | |
| Формы контроля (МК, экзамен, зачет) | МК, зачет | |
| Показатели | очная форма обучения | заочная форма обучения |
| Количество зачетных единиц (кредитов) | 3 | |
| Год подготовки | 1 | |
| Семестр | 1 | |
| Количество часов | 108 | |
| - лекционных | 18 | |
| - практических, семинарских | 18 | |
| - лабораторных | - | |
| - самостоятельной работы | 72 | |
| в т.ч. индивидуальное задание | - | |
| Недельное количество часов, | 6 | |
| в т.ч. аудиторных | 2 | |

## 3. ОПИСАНИЕ ДИСЦИПЛИНЫ

**Цели и задачи**

Целью освоения дисциплины «Современные проблемы прикладной математики и информатики» является получение базового представления о предпосылках появления распределенных реестров, возможностях и целях технологии блокчейн, основных математических алгоритмах и ряде систем, в которых используется данная технология, в том числе при создании и функционирования криптовалют.

К основным задачам данной дисциплины относятся:

- усвоение теоретических основ и практических навыков работы с распределенным реестром и использования технологии блокчейн в сфере обеспечения платежных систем, а также для других технологических процессов;
- освоение фундаментальных принципов построения и функционирования криптовалют и других распределенных систем на основе технологии блокчейн;
- понимание основных алгоритмов консенсуса, их ключевые свойства и характеристики, а также их применение;
- приобретение навыков работы с электронным кошельком, разработки и реализации различных скриптов и получение представления о смарт-контрактах;
- развитие навыков самостоятельной работы и умений находить и перерабатывать дополнительную информацию в данной предметной области;
- развитие творческого, научного потенциала студентов, их познавательных интересов в области математического и технологического обеспечения современных финансовых технологий, стимулирование к дальнейшему занятию научной деятельностью.

**Требования к результатам освоения дисциплины.** Процесс изучения дисциплины «Современные проблемы прикладной математики и информатики» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО РФ направления подготовки «01.04.02 Прикладная математика и информатика» и основной образовательной программы высшего профессионального образования направления подготовки «01.04.02 Прикладная математика и информатика» (магистерская программа: Прикладная математика и информатика):

**а)** ***общекультурных (ОК):***

- способность к абстрактному мышлению, анализу, синтезу (ОК-1);
- готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения (ОК-2);
- готовность к саморазвитию, самореализации, использованию творческого потенциала (ОК-3);

**б)** ***общепрофессиональных (ОПК):***

- готовность к коммуникации в устной и письменной формах на государственном языке ДНР и иностранном языке для решения задач профессиональной деятельности (ОПК-1);
- способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение (ОПК-3);
- способность использовать и применять углубленные знания в области прикладной математики и информатики (ОПК-4);
- способность использовать углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов (ОПК-5);

***в) профессиональных (ПК):***

**научно-исследовательская деятельность:**

- способность проводить научные исследования и получать новые научные и прикладные результаты самостоятельно и в составе научного коллектива (ПК -1);

- способность разрабатывать и анализировать концептуальные и теоретические модели решаемых научных проблем и задач (ПК_2);

**проектная и производственно-технологическая деятельность:**

- способность разрабатывать и применять математические методы, системное и прикладное программное обеспечение для решения задач научной и проектно-технологической деятельности (ПК-3);
- способность разрабатывать и анализировать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-4)

**организационно-управленческая деятельность:**

- способность управлять проектами, планировать научно-исследовательскую деятельность, анализировать риски, управлять командой проекта (ПК-5);
- способность разрабатывать и оптимизировать бизнес-планы научно-прикладных проектов (ПК-7);

**нормативно-методическая деятельность:**

- способность разрабатывать корпоративные стандарты и профили функциональной стандартизации приложений, систем, информационной инфраструктуры (ПК -8);

**консалтинговая деятельность:**

- способность разрабатывать аналитические обзоры состояния области прикладной математики и информационных технологий (ПК-11);

**консорциумная деятельность:**

- способность к взаимодействию в рамках международных проектов и сетевых сообществ в области прикладной математики и информационных технологий (ПК-12).

**В результате изучения учебной дисциплины студент должен:**

***знать:***

- различие между институциональными и неинституциональными подходами к формированию и хранению критической информации;
- неинституциональные механизмы формирования распределенного доверия на базе распределенных реестров;
- принципы работы алгортимов консенсуса;
- базовые механизмы и алгоритмы функционирования распределенных реестров;
- специальную терминологию, связанную с созданием и применением на практике технологии блокчейн, криптовалют, смарт-контрактов и коллективного инвестирования;
- возможности, преимущества и ограничения технологии распределенных реестров, а также перспективы их применения;
- основные принципы и требования, предъявляемые к проектированию современных платежных систем;
- сферы и особенности использования смарт-контрактов;

***уметь:***

- различать понятия токена и криптовалюты;
- ориентироваться в алгоритмах консенсуса и их особенностях;
- различать типы составляющих архитектуры Blockchain-сети и их функциональные возможности;
- использовать опыт применения систем электронных денег на практике;
- оценивать возможности использования распределенных реестров в рамках конкретных бизнес-моделей;
- использовать технологию блокчейн в разработке программных решений;

***владеть:***

- специальной технической терминологией в данной сфере;
- принципами построения Blockchain-сетей;

- навыками взаимодействия с электронными кошельками;
- навыками нахождения аналогий между поставленной задачей и уже существующими решениями;
- навыками эффективного общего анализа возможностей применения распределенных реестров для решения конкретных задач.

## 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

| Порядковый номер и тема | Краткое содержание темы |
|---|---|
| ***Содержательный модуль 1. Экономические основы и предпосылки создания криптовалют и технологии блокчейн*** | |
| **Тема 1.** Деньги и платежные системы. Виды платежных систем, история их развития. | Бартерная, монетная, бумажная и чековая платежные системы: преимущества и недостатки. Платежная система электронных кошельков. Причины появления концепции криптовалюты. |
| **Тема 2.** Концепция криптовалют. Экономический аспект биткоина. | Сущность биткоина как цифровой валюты и его свойства. Формирование стоимости биткоина: спрос и предложение. Социально-экономические факторы, влияющие на стоимость биткоина. |
| **Тема 3.** Виды систем управления. | Понятие управления. Виды систем управления: централизованная, децентрализованная и распределенная системы. Преимущества и недостатки. |
| **Тема 4.** Основы системы блокчейн | Концепция блокчейн. Основные свойства и преимущества блокчейн. |
| **Тема 5.** Бизнес-среда структуры блокчейн | Бизнес-среда структуры блокчейн, стадии процесса ее принятия и инвестиции |
| **Тема 6.** Модель автолизинга | Основные элементы системы автолизинга. Модель автолизинга на основе блокчейн |
| **Тема 7.** Значимые личности и компании системы блокчейн | Наиболее значимые личности в системе блокчейн. Компании, использующие блокчейн |
| ***Содержательный модуль 2. Архитектура и технологические аспекты распределенных реестров*** | |
| **Тема 8.** Криптографические основы криптовалют | Хеш-функции и цифровые подписи, их свойства и особенности применения на практике. Примеры построения простых криптовалют |
| **Тема 9.** Механизмы децентрализации Биткоина | Децентрализация в сети Биткоин. Механизмы достижения распределенного консенсуса. Стимулирование узлов сети: плата за создание блока и транзакционная комиссия. Понятие майнинга. |
| **Тема 10.** Транзакции Биткоина | Транзакции биткоина. Заголовок. Скриптовый язык биткоина и особенности его использования. MULTISIG. Примеры практического применения скриптов биткоина. Механизм присоединения новых узлов к сети. Ограничения, существующие в сети Биткоин. |
| **Тема 11.** Хранение и использование биткоинов | Способы хранения биткоинов: локальное хранение, холодное и горячее хранилища. Способы разделения секретного ключа на части. Особенности работы с онлайн-кошельками, биткоин-биржами, платежными |

| | |
|---|---|
| | сервисами. |
| **Тема 12.** Особенности майнинга. | Цели и сложности майнинга. Поколения аппаратного обеспечения для майнинга: центральные процессоры общего назначения, GPU, программируемые пользователем вентильные матрицы, ASIC. Экологические аспекты биткоин-майнинга. Пулы совместного майнинга: цели создания и особенности распределения вознаграждения. Стратегии, применяемые майнерами. |
| **Тема 13.** Основы анонимности | Понятие анонимности. Способы увеличения анонимности в сети Биткоин. Децентрализованное и централизованное микширование. Анонимная коммуникационная сеть Tor. |
| ***Содержательный модуль 3. Социальные факторы блокчейна и криптовалют: механизмы регулирования, возможности применения, перспективы развития*** | |
| **Тема 14.** Влияние общества, политики и законодательства на систему Биткоин | Договоренности, на которых основана система Биткоин: договоренность о правилах, истории, ценности. Программное обеспечение Bitcoin Core. Механизмы регулирования системы Биткоин со стороны правительства. |
| **Тема 15.** Альтернативы Proof of Work | Особенности алгоритмов PoW и требования к ним. Альтернативные алгоритмы: алгоритмы с защитой от ASIC, алгоритмы, препятствующие объединению в пулы, социально полезные алгоритмы. Особенности вычисления Scrypt. Виртуальный майнинг: достоинства, недостатки, перспективы развития. |
| **Тема 16.** Практика использования Биткоина в разных областях | Безопасное проставление штампа времени: особенности применения и реализации. Практическое применение свойств Биткоина: организация и проведение лотерей, билеты, цветные монеты. Сущность рынка прогнозов и анализ возможности его построения на базе Биткоина. |
| **Тема 17.** Экосистемы криптовалют | Примеры альткоинов: неймкоин, лайткоин, пиркоин, догикоин. Способы сравнения альткоин-бирж и особенности их работы. Сущность совместного майнинга. Атомарные свопы как метод обмена разных альткоинов. |
| **Тема 18.** Будущее Биткоина | Статус системы блокчейн, перспективы развития. Умная собственность. Репрезентация и атомарность. Пути интеграции блокчейн: прямое использование блокчейн, встраивание, сайдчейн, альткоины. Реализация краудфандинга с помощью технологии блокчейн. Плюсы и минусы децентрализованных технологий в сравнении с традиционной системой. |

**Тематический план**

| Названия содержательных модулей и тем | Количество часов | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Очная форма обучения | | | | | | Заочная форма обучения | | | | | |
| | всего | в т.ч. | | | | | всего | в т.ч. | | | | |
| | | лекции | практические | лабораторные | самостоятельная работа | индивидуальная работа | | лекции | практические | лабораторные | самостоятельная работа | индивидуальная работа |
| **Тема 1.** Деньги и платежные системы. Виды платежных систем, история их развития. | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 2.** Концепция криптовалют. Экономический аспект биткоина. | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 3.** Виды систем управления. | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 4.** Основы системы блокчейн | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 5.** Бизнес-среда структуры блокчейн | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 6.** Модель автолизинга | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 7.** Значимые личности и компании системы блокчейн | **6** | 1 | 1 | | 4 | | | | | | | |
| ***Итого по содержательному модулю 1*** | **42** | 7 | 7 | | 28 | | | | | | | |
| **Тема 8.** Криптографические основы криптовалют | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 9.** Механизмы децентрализации Биткоина | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 10.** Транзакции Биткоина | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 11.** Хранение и использование биткоинов | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 12.** Особенности майнинга. | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 13.** Основы анонимности | **6** | 1 | 1 | | 4 | | | | | | | |
| ***Итого по содержательному модулю 2*** | **36** | 6 | 6 | | 24 | | | | | | | |
| **Тема 14.** Влияние общества, политики и законодательства на систему Биткоин | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 15.** Альтернативы Proof of Work | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 16.** Практика использования Биткоина в разных областях | **6** | 1 | 1 | | 4 | | | | | | | |
| **Тема 17.** Экосистемы криптовалют | **6** | 1 | 1 | | 4 | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Тема 18.** Будущее Биткоина | **6** | 1 | 1 | | 4 | | | | | | | |
| ***Итого по содержательному модулю 3*** | **30** | 5 | 5 | | 20 | | | | | | | |
| ***Всего по дисциплине*** | **108** | 18 | 18 | | 72 | | | | | | | |

## 5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

### Темы лекционных занятий

| *№ п/п* | *Название темы* | *Количество часов* |
|---|---|---|
| 1 | Деньги и платежные системы. Виды платежных систем, история их развития. | 1 |
| 2 | Концепция криптовалют. Экономический аспект биткоина. | 1 |
| 3 | Виды систем управления. | 1 |
| 4 | Основы системы блокчейн | 1 |
| 5 | Бизнес-среда структуры блокчейн | 1 |
| 6 | Модель автолизинга | 1 |
| 7 | Значимые личности и компании системы блокчейн | 1 |
| 8 | Криптографические основы криптовалют | 1 |
| 9 | Механизмы децентрализации Биткоина | 1 |
| 10 | Транзакции Биткоина | 1 |
| 11 | Хранение и использование биткоинов | 1 |
| 12 | Особенности майнинга. | 1 |
| 13 | Основы анонимности | 1 |
| 14 | Влияние общества, политики и законодательства на систему Биткоин | 1 |
| 15 | Альтернативы Proof of Work | 1 |
| 16 | Практика использования Биткоина в разных областях | 1 |
| 17 | Экосистемы криптовалют | 1 |
| 18 | Будущее Биткоина | 1 |
| | **ВСЕГО** | **18** |

### Темы практических занятий

| *№ п/п* | *Название темы* | *Количество часов* |
|---|---|---|
| 1 | Основные элементы системы Биткоин и блокчейн | 1 |
| 2 | Исследование структуры блокчейна с помощью Blockchain Explorer | 1 |
| 3 | Структура блока блокчейна Биткоин | 1 |
| 4 | Структура транзакций | 1 |
| 5 | Струкутры данных для представления элементов блокчейна | 1 |
| 6 | Приложение Bitcoin Core и его возможности | 1 |
| 7 | Тестовые сети Биткоина | 1 |
| 8 | Клиентские приложения и их основные возможности | 1 |

| | | |
|---|---|---|
| 9 | Алгоритмы хеширования семейства SHA | 1 |
| 10 | Шифрование с открытым ключом | 1 |
| 11 | Генерация ключей. Механизмы создания подписей | 1 |
| 12 | Задача Proof of Work. Оценка сложности | 1 |
| 13 | Майнинг | 1 |
| 14 | Получение истории транзакций и баланса транзакций | 1 |
| 15 | Криптовалюта Ethereum. Структура и операции в Ethereum | 1 |
| 16 | Смарт-контракты. Язык Solidity | 1 |
| 17 | Разработка смарт-контрактов в Remix IDE | 1 |
| 18 | Развертывание смарт-контрактов | 1 |
| | **ВСЕГО** | **18** |

## 6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

### Организация самостоятельной работы студентов

| *№ п/п* | *Название темы* | *Количество часов* |
|---|---|---|
| 1 | Технология блокчейн и децентрализованные приложения | 4 |
| 2 | Приватные и публичные блокчейны | 4 |
| 3 | Сравнительная характеристика традицинных банковский онлайн-транзакций и транзакций в сети Биткоин | 4 |
| 4 | Полные ноды и облегченные кошельки в сети Биткоин | 4 |
| 5 | Блокчейн и его возможности | 4 |
| 6 | Токенизация и ICO | 4 |
| 7 | Формат ключей в Биткоин | 4 |
| 8 | Форки Биткоина | 4 |
| 9 | Хранение и обработка ключей в криптовалютных кошельках | 4 |
| 10 | Иерархическая генерация ключей | 4 |
| 11 | Pay-to-Script-Hash адреса и иультиподписи в Биткоин | 4 |
| 12 | Альтернативные форматы представления биткоин-адресов | 4 |
| 13 | Жизненный цикл транзацкий | 4 |
| 14 | Протокол Segregated Witness | 4 |
| 15 | Обмен сообщениями между узлами Биткоин-сети | 4 |
| 16 | Технологии повсеместной токенизации | 4 |
| 17 | Виды атак и решения для их предотвращения в Биткоин | 4 |
| 18 | Методы построения криптографических обязательств | 4 |
| | **ВСЕГО** | **72** |

## 7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

### Индивидуальная работа
### *СТРУКТУРА БЛОКЧЕЙНА БИТКОИНА И ЯЗЫК BITCOIN SCRIPT*

**Цель:** получение практических навыков работы с блокчейном Биткоина, анализа характеристик различных блоков и транзацкий и создания сценариев на языке Bitcion Script

**Задания:**

1. Определите время создания и хеш блока в основной цепочке блокчейна Биткоин, находящегося на высоте N=350738.
2. Определите время создания и высоту блока со значением хеша 000000000a529eeb7c75b4faca15f48ef712eb70ce6dc28b8c4df5c907c19bb4.
3. Определите количество транзакций в блоке на высоте 364077 и хеш coinbase-транзакции этого блока.
4. Определите хеш блока на высоте 296878 и по запакованной версии цели bits максимальное допустимое значение хеша этого блока. Убедитесь в том, что хеш не превышает максимально допустимого значения.
5. Определите высоту блока, в котором находится транзакция со значением хеша 2d6bac2ef23e771b018870ca5f06948fd9f06648a0eeaaa91dda78a9b3c71684, количество ее входов и выходов, их стоимость, а также связанные с ними адреса.
6. С помощью калькулятора https://cse.buffalo.edu/blockchain/blockhash.html проверьте для блока, находящегося на высоте 313682, корректность вычисления его хеша. Данные для отметки времени вводите с учетом вашего текущего часового пояса. Подберите любое другое значение nonce для этого блока, которое обеспечивает значение хеша с совпадающими двумя первыми шестнадцатеричными цифрами.
7. Для каждого входа транзакции со значением хеша c659f0dab6b93600467372ee5563af8e2100ed5548559cb1275cf02b2afcb4fa укажите, в какой транзакции был получен соответствующий данному входу выход (хеш транзакции) и номер этого выхода (выходы нумеруются с нуля).
8. Напишите сценарий на Bitcoin Script, который упорядочивает по неубыванию три верхних значения в стеке.

## 8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Перечислите наиболее желательные свойства денег. Какими из этих свойств обладают деньги в различных платежных системах.
2. Должны ли деньги обязательно иметь внутреннюю стоимость?
3. В результате чего появляются долговые отношения в примитивных обществах?
4. Какие функции выполняют деньги в соответствии с законодательством о банковской системе?
5. С чем связана проблема двойной траты в системах электронных платежей и криптовалютах?
6. Назовите основные механизмы формирования стоимости криптовалют.
7. Опишите механизм одобрения транзакций в сети Биткоин.
8. В чем заключается идея распределенного консенсуса?
9. Укажите основные характеристики системы Биткоин, которые поддерживаются программным обеспечением и участниками сети.
10. Перечислите виды систем относительно типа управления, принятого в них. Укажите преимущества и недостатки каждого типа управления.
11. Перечислите основные требования, которые предъявляются к хеш-функциям.
12. Опишите механизм обязательств, построенных с использованием электронной подписи и хеша.
13. Что такое хеш-указатель и как он используется при формировании блоков?
14. Опишите структуру дерева Меркла и его основные свойства.
15. Опишите процесс майнинга, какую задачу должен решать майнер для получения вознаграждения?
16. В чем заключается идея холодного и горячего хранилища?
17. На чем основана концепция разделения ключей? Опишите ее механизм.
18. Перечислите преимущества и недостатки онлайн-кошелька.

19. Для чего майнеры объединяются в пулы и на каких принципах осуществляется их деятельность?

20. Приведите примеры кейсов в которых удобно использовать переадресацию, слепые подписи, зеленые адреса, микротранзакции, мультиподписи.

## 9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

**ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»**

Факультет математики и информационных технологий

| | |
|---|---|
| *Направление подготовки:* | ***01.04.02 Прикладная математика и информатика*** |
| *Магистерская программа:* | ***Прикладная математика и информатика*** |
| *Программа подготовки:* | ***академическая магистратура*** |
| *Семестр* | ***1*** |
| *Учебная дисциплина* | ***Современные проблемы прикладной математики и информатики*** |

**МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА, Часть 1**
**ВАРИАНТ №1**

1. В каком году были определены и опубликованы протокол и принципы работы системы Биткоин?
2. Какой из видов платежных систем обеспечивает самую высокую скорость проведения платежей?
3. Перечислите преимущества и недостатки бартерной платежной системы.
4. В чем основной недостаток платежной системы электронных кошельков?
5. В каком случае транзакция в сети Биткоин считается одобренной?
6. Каким числом может выражаться величина платежа в системе Биткоин?
7. Перечислите основные социально-экономические факторы, влияющие на стоимость биткоина.
8. Охарактеризуйте процесс майнинга с точки зрения наличия конкуренции и типа управления.
9. Как называется власть или право отдавать приказы, принимать решения и требовать повиновения?
10. К какому типу систем относится банковская система Донецкой Народной Республики?
11. Назовите основные преимущества централизованных систем управления.
12. Охарактеризуйте систему блокчейн с точки зрения посредников, иерархии, доверия и режима доступа к информации (ее чтения/записи).
13. Где гранится информация о страховке машины в схеме автолизинга на основе блокчейн?
14. Что достоверно известно о личности Сатоши Накамото?
15. Чем занимается компания Lazooz?

**МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА, Часть 2**
**ВАРИАНТ №1**

1. Охарактеризуйте множество результатов вычисления хеш-функции.
2. Как называется свойство защищенной хеш-функции, которое исключает что кто-то из хеш-функции получит определенное выходное значение y?
3. Что необходимо сделать злоумышленнику, если он хочет подделать данные в одном из блоков дерева Меркла?
4. Как должен поступить узел в рамках работы протокола распределенного консенсуса, если он получил блок, который содержит транзакции с корректными криптографическими подписями?
5. Укажите причины, по которым Биткойн способен достичь консенсуса на практике, вопреки тому, что в общем это довольно сложная задача?

6. Как в терминах сценариев проверяется то, что транзакция может быть успешно завершена?
7. Какие группы инструкций поддерживает скриптовый язык Биткоина?
8. Элис платит за услугу Бобу, используя микротранзакции. Если она внезапно отключится, не предупредив Боба, и перестанет пересылать оплату, что может сделать Боб в такой ситуации?
9. Как должны быть распределены средства между горячим и холодным хранилищем?
10. Биржа публикует валидную транзакцию с переводом 10 000 биткоинов сама на себя. Затем биржа подписывает случайно сгенерированную строку своим закрытым ключом, которым была подписана предыдущая транзакция в 10 000 биткоинов. Зачем это делается?
11. Какие основные факторы необходимо учитывать при определении рентабельности майнинга?
12. Что может означать несвязанность в Биткойн?
13. В каком случае пользователь сети Tor может потерять безопасность передачи информации по цепи маршрутизаторов?
14. Какой механизм использовал Шелковый путь, чтобы мотивировать участников на ведение честных сделок?
15. Перечислите требования к алгоритмам Proof of work.

Утверждено на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского, протокол № ___ от «_____» _____ 20_____ г.

Заведующий кафедрой _____
Преподаватель _____

**Критерии оценивания модульного контроля**

| ***Номер задания*** | ***Количество баллов*** |
|---|---|
| часть 1, 1-15 | по 2 балла |
| часть 2, 1-15 | по 2 балла |
| ***Всего*** | ***60 баллов*** |

## 10. КРИТЕРИИ ОЦЕНИВАНИЯ

По курсу предполагается проведение промежуточной аттестации в виде модульного контроля, состоящего из двух частей, выполнения индивидуальной работы и зачета.

Индивидуальная работа оценивается исходя из максимальных 30 баллов. Каждая из частей модульного контроля содержит тестовое задание, состоящее из 15 вопросов по различным темам, и оценивается исходя из максимальных 30 баллов. Индивидуальная творческая работа студентов предполагает подготовку доклада или реферата на одну из тем, представленных в разделе 6 настоящей рабочей программы, и оценивается в 10 баллов.

Зачет сдают студенты с целью повышения рейтинга. Оценка за семестр вычисляется как максимальная из полученных за семестр и на зачете и выставляется согласно шкале, принятой в ДонНУ.

***Распределение баллов, которые могут получить студенты в процессе изучения дисциплины***

| **Организационно учебная работа студента** | **СРС** | | | **Всего** |
|---|---|---|---|---|
| | **Индивидуальная работа** | **Модульный контроль** | **Индивидуальная творческая работа** | |
| Max 0 баллов | max 30 баллов | max 60 баллов | max 10 баллов | 100 баллов |

| | | | | |
|---|---|---|---|---|
| | | | подготовка доклада или реферата | |

***Шкала соответствия баллов национальной шкале***

| Оценка по шкале ECTS | Оценка по 100-балльной шкале | Оценка по государственной шкале (экзамен, дифференцированный зачет) | Оценка по государственной шкале (зачет) |
|---|---|---|---|
| **A** | 90-100 | 5 (отлично) | зачтено |
| **B** | 80-89 | 4 (хорошо) | зачтено |
| **C** | 75-79 | 4 (хорошо) | зачтено |
| **D** | 70-74 | 3 (удовлетворительно) | зачтено |
| **E** | 60-69 | 3 (удовлетворительно) | зачтено |
| **FX** | 35-59 | 2 (неудовлетворительно) с возможностью повторной сдачи | не зачтено |
| **F** | 0-34 | 2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов | не зачтено |

## 11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Лекционные занятия проводятся в аудитории, оснащенной (мультимедийной техникой и) доской. Практические занятия выборочно проводятся в компьютерном классе, оборудованном компьютерами с лицензионным программным обеспечением, доступом к сети Интернет, столами, доской.

## 12. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

| № п/п | Наименование | Кол-во экземпляров в библиотеке ДонНУ | Наличие электронной версии в ЭБС |
|---|---|---|---|
| | ***Основная литература*** | | |
| 1. | Дрешер Д. Основы блокчейна: вводный курс для начинающих в 25 небольших главах / Даниэль Дрешер. – М.: ДМК Пресс, 2018. - 312 с.: ил. | 0 | 0 |
| 2. | Генкин А, Алексей Михеев А. Блокчейн. Как это работает и что ждет нас завтра / Артем Генкин, Алексей Михеев. – М.: Издательство Альпина Паблишер, 2018. - 592 с. | 0 | 0 |
| 3. | Романьков, В.А. Введение в криптографию. Курс лекций / В.А. Романьков. – 2-е изд., испр. и доп. – М.: ФОРУМ : ИНФРА-М, 2018. – 240 с. | 0 | 0 |
| | ***Дополнительная литература*** | | |
| 4. | Свон М. Блокчейн: схема новой экономики / Мелани Свон. - М.: Олимп-бизнес, 2017. - 240 с., ил. | 0 | 0 |
| 5. | Равал С. Децентрализованные приложения. Технология Blockchain в действии / С.Равал. – СПб.: Питер, 2017. – 240 с.: ил. | 0 | 0 |
| 6. | Поппер Н. Цифровое Золото. Невероятная история биткойна или о том, как идеали-сты и бизнесмены | 0 | 0 |

| | | | |
|---|---|---|---|
| | изобретают деньги заново / Натаниэль Поппер. - М.: Диалектика, 2016. - 75 с. | | |
| 7. | Винья П., Майкл Кейси М. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок / Пол Винья, Майкл Кейси. - М.: Издательство Манн, Иванов и Фербер. 2017. - 432 с. | 0 | 0 |

## 13. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Онлайн-курс «Введение в криптовалюты и блокчейн» // Intuit.ru – URL: https://www.intuit.ru/studies/courses/3443/685/info
2. Онлайн-курс «Технологии криптовалют» // Intuit.ru – URL: https://www.intuit.ru/studies/courses/3643/885/info
3. Серия публикаций Bitcoin in a nutshell // Хабрахабр:
   Cryptography - https://habrahabr.ru/post/319868/
   Transaction - https://habrahabr.ru/post/319860/
   Protocol - https://habrahabr.ru/post/319862/
   Blockchain - https://habrahabr.ru/post/320176/
   Mining - https://habrahabr.ru/post/320178/
4. Курс лекций от группы Distributed Lab // Youtube. – URL: https://www.youtube.com/playlist?list=PLhZQuknA7yUBt82ow8rEfw_G8tNZjt3qB
5. Bitcoin Wiki – URL: https://en.bitcoin.it/wiki/Introduction
6. Официальная документация Bitcoin Core: https://bitcoin.org/en/developer-documentation
7. Bitcoin Whitepaper: http://www.bitcoin.org/bitcoin.pdf
8. Bitcoin's Academic Pedigree: https://queue.acm.org/detail.cfm?id=3136559
9. What is Blockchain Technology? A Step-by-Step Guide For Beginners https://blockgeeks.com/guides/what-is-blockchain-technology
10. Blockchain: The Invisible Technology That's Changing the World https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor
11. How a Bitcoin Transaction Works https://www.ccn.com/bitcoin-transaction-really-works/
12. A Gentle Introduction to Blockchain Technology https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/
13. On Public and Private Blockchain https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
14. What is Cryptocurrency. Guide for Beginners https://cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies#accept-as-payment-for-business
15. 2017 Was Bitcoin's Year. 2018 Will Be Ethereum's https://www.coindesk.com/2017-bitcoins-year-2018-will-ethereums/
16. What is Cryptocurrency: Everything You Need To Know https://blockgeeks.com/guides/what-is-cryptocurrency/
17. Smart Contracts: The Blockchain Technology That Will Replace Lawyers https://blockgeeks.com/guides/smart-contracts/
18. Introduction to Smart Contracts http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html
19. What is Ethereum? http://ethdocs.org/en/latest/introduction/what-is-ethereum.html
20. Smart Contracts: A White Paper https://github.com/ethereum/wiki/wiki/White-Paper
21. Account Management http://ethdocs.org/en/latest/account-management.html
22. Native: Account management https://github.com/ethereum/go-ethereum/wiki/Native:-Account-management
23. How Ethereum Works https://www.coindesk.com/information/how-ethereum-works/

24. What Is Meant By The Term “Gas”? https://ethereum.stackexchange.com/questions/3/what-is-meant-by-the-term-gas
25. Vitalik Buterin Doubles Down on Ethereum Incentive Strategy https://www.coindesk.com/vitalik-buterin-doubles-ethereum-incentive-strategy
26. Blockchain Info https://blockchain.info/
27. Bitcoin Block Explorer https://blockexplorer.com/
28. Etherscan https://etherscan.io/

## 14. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Веб-браузер Google Chrome (Лицензия – бесплатное программное обеспечение с открытым исходным кодом) – URL: https://www.google.com/intl/ru/chrome/
2. Bitcoin Core (свободный проект с открытым исходным кодом, лицензия MIT) – URL: https://bitcoin.org/ru/download
3. Remix IDE (свободный проект с открытым исходным кодом, лицензия MIT) – URL: https://remix.ethereum.org

Рабочая программа рассмотрена и переутверждена на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского с изменениями (без изменений) на 20____ год.

Протокол № ___ от “___” __________ 20__ г.

Заведующий. кафедрой ______________ В.И. Сторожев

Рабочая программа рассмотрена и переутверждена на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского с изменениями (без изменений) на 20____ год.

Протокол № ___ от “___” __________ 20__ г.

Заведующий. кафедрой ______________ В.И. Сторожев

Рабочая программа рассмотрена и переутверждена на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского с изменениями (без изменений) на 20____ год.

Протокол № ___ от “___” __________ 20__ г.

Заведующий. кафедрой ______________ В.И. Сторожев

Рабочая программа рассмотрена и переутверждена на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского с изменениями (без изменений) на 20____ год.

Протокол № ___ от “___” __________ 20__ г.

Заведующий. кафедрой ______________ В.И. Сторожев