МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
Декан _____ Буднев Н.М.
«22» апреля 2020 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) **Б1.В.03 Распределенные базы данных. Блокчейн**

Направление подготовки 10.03.01 Информационная безопасность

Тип образовательной программы бакалавриат

Направленность (профиль) подготовки №4 Безопасность автоматизированных систем (в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

1. Цели и задачи дисциплины (модуля)

Развитие цифровых технологий привело к изменению концепции хранения и обработки данных в сети. Одним из современных направлений стала разработка NoSQL баз данных. При создании такой базы данных не требуется соблюдения формальных правил разработки таблиц. Информация хранится в так называемых плоских файлах в виде пар «параметр-значение».

Курс знакомит с современными методами хранения и обработки данных на примере распределенной базы данных – блокчейна. Информация в этой базе данных сохранена в непрерывной последовательной цепочке блоков, связанных между собой.

Разобраны криптографические алгоритмы, применяемые для блокчейна, рассмотрено создание и функционирование блокчейна на примере криптовалют. Приведены примеры программирования работы сети, обслуживающей криптовалюту.

.

2. Место дисциплины в структуре ОПОП

Курс рассчитан на бакалавров физических специальностей университетов. Является продолжением информатики, которую студенты усваивают на младших курсах и курса «Базы данных». Таким образом, обеспечивается непрерывность компьютерного образования. Занятия рассчитаны на один семестр.

Практические занятия предполагают работу на компьютерах и включают знакомство с криптографическими алгоритмами и работой в сети.

Курс «Распределенные базы данных. Блокчейн» относится к части, формируемой участниками образовательных отношений. Он изучается в пятом семестре на третьем курсе бакалавриата.

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

ОПК-1 - способностью анализировать физические явления и процессы для решения профессиональных задач

ПК-11 способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

В результате изучения дисциплины студент должен:

Знать: принципы построения распределенных баз данных на основе блокчейна,

основные методы проектирования этих баз данных и их применения для хранения данных в сети.

Уметь: проектировать и программировать эти системы и использовать их для хранения данных.

Владеть: инструментами программирования блокчейна и навыками грамотного использования существующих систем криптовалют

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	**Всего часов / зачетных единиц**	**Семестры**			
		5			
Аудиторные занятия (всего)	100/2,7	100/2,7			
В том числе:	-	-	-	-	-
Лекции	50/1,4	50/1,4			
Практические занятия (ПЗ)	34/0,9	34/0,9			
Семинары (С)					
Лабораторные работы (ЛР)	16/0,4	16/0,4			
КСР					
Самостоятельная работа (всего)	98/2,7	98/2,7			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы	98/2,7	98/2,7			
Вид промежуточной аттестации (*зачет, экзамен*)	экзамен	экзамен			
Контактная работа (всего)	100/2,7	100/2,7			
Общая трудоемкость часы	252	252			
зачетные единицы	7	7			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

Раздел 1. Криптографические алгоритмы.

Тема 1. Алгоритмы хеширования. Алгоритм хеширования SHA256. Алгоритм хеширования RIPEMD160.

Тема 2. Криптография на эллиптических кривых. Непрерывная группа точек на эллиптической кривой. Дискретная группа точек. Модулярная арифметика. Длинная арифметика. Циклическая подгруппа.

Тема 3. Электронный кошелек. Алгоритм вычисления открытого и закрытого ключа. Создание электронного адреса. Кодировка Base58Check. Электронная подпись. Проверка подписи.

Раздел 2. Учебная криптовалюта.

Тема 4. Структура блока. Создание нового блока. Майнинг.

Тема 5. Транзакции. Структура транзакции. Создание транзакции. Проверка правильности транзакции.

Тема 6. Структура сети для работы с блокчейном. Технология P2P. Схема работы узла сети.

Раздел 3. Биткоин.

Тема 7. Структура блока. Генезис – блок.

Тема 8. Транзакции. Хеширование транзакций. Подтверждение транзакций.

Тема 9. Биткоин-кошелек и биткоин-адрес.

Тема 10. Майнинг. Алгоритм доказательства работы. Форки блокчейна.

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Базы данных	1-10
2	Электротехника	1-10
3	Основы построения и функционирования специальных технических средств	1-10
4	Безопасность компьютерных сетей	1-10
5	Практика по получению первичных профессиональных	1-10

	умений и навыков	
6	Эксплуатационная практика	1-10
7	Проектно-технологическая практика	1-10

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1	5	3		1	8	17
2.	***Раздел 1***	Тема 2	5	3		1	10	19
3.	***Раздел 1***	Тема 3	5	3		2	10	20
4.	***Раздел 2***	Тема 4	5	3		1	10	19
5.	***Раздел 2***	Тема 5	5	4		2	10	21
6	***Раздел 2***	Тема 6	5	4		2	10	21
7	***Раздел 3***	Тема 7	5	4		2	10	21
8	***Раздел 3***	Тема 8	5	4		2	10	21
9	***Раздел 3***	Тема 9	5	3		2	10	20
10	***Раздел 3***	Тема 10	5	3		1	10	19

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 1***	Лабораторная №1	13	Тестовый контроль по теме	ОПК-1
2.	***Раздел 2***	Лабораторная №2	16	Тестовый контроль по теме	ОПК-1
3.	***Раздел 3***	Лабораторная №3	21	Тестовый контроль по теме	ПК-11

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	**1-3**	Подготовка к контрольной	№1	Учебный сайт	49

		работе №1			
8		Контрольная работа №1.		Учебный сайт	
9		Подведение итогов по контрольной работе №1. Работа над ошибками по контрольной работе №1.		Учебный сайт	
10-16	**4-5**	Подготовка итоговой зачетной работы	№2	Учебный сайт	49
17		Подготовка доклада с презентацией		Учебный сайт	
18		Подведение итогов		Учебный сайт	

6.2. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, в ходе которой студент активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи. Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

В процессе проведения самостоятельной работы формируется компетенция ОПК-7

Контроль самостоятельной работы на лабораторных занятиях и на КСР, по окончании соответствующих тем.

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

основная литература

1. Красов, В.И. Распределение базы данных Блокчейн [Текст] : учеб. пособие / В. И. Красов ; Иркут. гос. ун-т, Физ. фак. - Иркутск : Изд-во ИГУ, 2020. - 118 с. : ил., табл. ; 20 см. - Библиогр.: с. 107. - ISBN 978-5-9624-1848-3 – (20 экз.)

дополнительная литература

1. Макшанов, А. В. Большие данные. Big Data [Текст] : учебник / А. В. Макшанов, А. Е. Журавлев, Л. Н. Тындыкарь. - СПб. : Лань, 2021. - 184 с. : ил. ; 24 см. - (Высшее образование). - Библиогр.: с. 181-184. - ISBN 978-5-8114-6810-2. – (11 экз).

б) *периодические издания*

- нет.

в) *список авторских методических разработок*

1. *В.И.Красов*. Распределенные базы данных. Блокчейн. — Иркутск: изд. ИГУ, 2020. – 118 с. - Режим доступа: ЭЧЗ "Библиотех". - Неогранич. доступ.

2. В системе образовательного портала ИГУ (http://educa.isu.ru/) размещены методические материалы и задания по данному курсу.

г) *базы данных, информационно-справочные и поисковые системы*

документация, описание и примеры работы Блокчейн:

- https://blockgeeks.com/guides/what-is-blockchain-technology/
- https://bitcoin.org
- https://github.com/bitcoin/bitcoin
- Blockchain University - - https://www.youtube.com/channel/UCJ5uHx90mZGlK0lC-GSmtzw
  - Blockchain Workshops? - https://www.youtube.com/channel/UC9Lmf5FfNkSmYMoxhQh5ktA/feed
  - Что такое блокчейн-технология? - https://bitnovosti.com/2017/03/02/chto-takoe-tehnologija-blokchein-posagovoe-rukovodstvo-dlja-novichkov-1
- • ЭЧЗ «Библиотех» https://isu.bibliotech.ru/
- • ЭБС «Лань» http://e.lanbook.com/
- • ЭБС «Руконт» http://rucont.ru
- • ЭБС «Айбукс» http://ibooks.ru

Справочные материалы:

1. *Lauri Hartikka*. Naivecoin: a tutorial for building a cryptocurrency [Электронный ресурс]. https://lhartikk.github.io/jekyll/update/2017/07/14/chapter1.html

2. *S. Nakamoto*, Bitcoin Whitepaper. [Электронный ресурс] URL: https://bitcoin.org/bitcoin.pdf - (Дата обращения: 17.07.2019)

3. Protocol documentation [электронный ресурс]. – URL: https://en.bitcoin.it/wiki/Protocol_documentation

4. Buterin V.et al.A next-generation smart contract and decentralized application platform //white paper. –2014. URL:https://github.com/ethereum/wiki/wiki/White-Paper (accessed 29 October 2018)

9. Материально-техническое обеспечение дисциплины (модуля)

Применять полученные знания на практике студенты могут в специальном дисплейном классе с современной вычислительной техникой и соответствующим программным обеспечением. В классе имеет 14 стационарных компьютеров (Intel Atom CPU D2500) с мониторами (Samsung S19A10 18.5"), WiFi-роутер 54M Wireless Router TL-WR542G, маршрутизатор DES-1005D. Компьютеры имеют доступ к локальной сети университета и выход в Интернет. Студенты могут самостоятельно закреплять полученный материал в этих классах. На занятиях могут использоваться мультимедийные средства: переносной проектор (CASIO XJ-A241), стационарный настенный экран (Classic Solution, 244x244), ноутбук Lenovo B590. Кроме того, на факультете имеется компьютеризированная аудитория, предназначенная для самостоятельной работы.

10. Образовательные технологии

Для достижения планируемых результатов обучения, «Веб-программирование» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении

экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения химических исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем общей и неорганической химии на лекциях, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Входной контроль не осуществляется.

11.2. Оценочные средства текущего контроля

Контроль за работой студентов осуществляется посредством собеседования при защите ими отчетов по лабораторным работам.

Ниже приведены задания к некоторым разделам программы.

Задания к разделу 1

1. Написать программу, вычисляющую хеш от произвольного текста по адгоритму SHA256, сравнить с образцом, рассчитанным online – калькулятором в интернете.
2. Написать программу, вычисляющую хеш от произвольного текста по формату RIPMD160, сравнить с образцом, рассчитанным online – калькулятором в интернете.
3. Рассчитать и изобразить эллиптические кривые с параметрами: b=1, a = 2 -3.
4. Написать программу сложения двух точек эллиптической кривой. Проверить алгоритм на графике.
5. Написать программу вычисления остатка от деления целого числа на заданный модуль для положительных и отрицательных чисел.
6. Написать программу поиска мультипликативной инверсии числа в поле Fp с и использованием расширенного алгоритма Эвклида.
7. Написать программу нахождения частного от деления двух целых чисел в модулярной арифметике.
8. Вычислить все точки, принадлежащие группе точек эллиптической кривой по модулю p<1000. Изобразить на графике.
9. Написать программу вычисления скалярного произведения точки на число методом удвоения – сложения.
10. Определить циклическую подгруппу, выбрав базовую точку из точек, принадлежащих некоторой группе на эллиптической кривой (см. задание 1).
11. Написать программу перекодировки произвольного длинного числа из 16-ричного формата (строки байтов) в формат Base58.
12. Написать программы раскодировки, т.е. перевода строки формата Base58 в 16-ричный формат.
13. Используя стандартные криптографические библиотеки написать программу получения электронной подписи и ее проверки.

Задания к разделу 2

1. Написать программу создания нового блока для криптовалюты, используя стандартные криптографические библиотеки. Промоделировать майнинг, создавая блоки с заданным условием на значение хеша.

2. Написать программу для создания транзакции.

3. Практическая работа в сети для учебной криптовалюты.

Задания к разделу 3

1. Получить последний блок на сайте «blockchain.info» , посмотреть структуру, значения констант сложность, nonce, количество нулей в хеше.

2. Получить транзакцию из этого блока (любую), посмотреть скрипты, расшифровать их.

Примерный список вопросов к зачёту:

- Блокчейн. Дайте определение. Каковы его свойства? Приведите примеры.
- Какие типы блокчейнов существуют?
- Что такое задача консенсуса?
- Какими свойствами обладает консенсус, основанный на доказательстве выполнения работы?

- Доказательство выполнения работы в сети Биткоин.
- Как устроен криптографический алгоритм с открытым ключом RSA?

- Сформулируйте задачу доказательства с нулевым разглашением.
- Как устроен алгоритм разделения секрета по схеме Шамира?
- Криптографические хэш функции.
- Задача консенсуса. Теорема FLP.

- Микроплатежи и умные контракты
- Какие возможности есть в языке Биткоин скрипт?
- Как устроены микроплатежи в Биткоине?
- Как устроен язык Солидити?

- Что такое византийски устойчивые алгоритмы консенсуса?
- Какие типы сетей и процессоров выделяют в задаче византийски устойчивого консенсуса?
- Архитектура фремворка Экзонум.

- Как устроен консенсус с делегированным доказательством обладания долей?
- Какую блокчейн и оффчейн информацию можно извлечь о сети Биткион?
- Что такое приватный умный контракт?

Пример тестовых заданий для проверки сформированности компетенций, указанных выше п.III:

1. Приведены четыре дайджеста, полученных хешированием различных текстов методом SHA256. Какой из них ошибочный?

1) 6ed2cf20c6231a153fc3959fc10bbe8923f4bb9402cdbef7f1807a6b301b0437

2) 4ae7c3b6ac0beff671efa8cf57386151c06e58ca53a78d8uf36107316cec125f

3) c9c9df56e2529684f8742be7c27d9fc47c2ec708d50342297cc2e43faf90d822

4) 4afe0b28a14803a191c75e35a383e58d9e890dffe6a0e80277c5f2a244b1990c

2. Что является суммой двух точек на эллиптической кривой.

1) Точка, координаты которой равны сумме координат двух точек.

2) Точка, обратная точке, в которой эллиптическая кривая пересекается линией, соединяющей заданные две точки.

3) Точка, координаты которой равны разности координат двух точек.

4) Точка эллиптической кривой, образующая с первыми двумя равносторонний треугольник.

3. Что представляет собой приватный адрес?

1) Случайное 256- битное число.

2) Номер в списке пользователей блокчейна

3) Хеш фамилии пользователя.

4) Название группы пользователей блокчейна

4. Что такое майнинг?

1) Поиск спрятанных в сети денег.

2) Договор с пользователями блокчейна о распределении криптовалюты

3) Обслуживание пользователей блокчейна за определенный гонорар.

4) Создание нового блока, хеш которого меньше заданного числа.

5. Как обеспечивается надежная связь между блоками с данными в блокчейне?

1) Использование электронной подписи

2) Организация прав доступа пользователей

3) Добавление в состав блока хеша предыдущего блока

4) Шифрование информации

6. Что такое транзакции?

1) Состояние блокчейна на текущий момент

2) Записи о движении криптовалюты между кошельками

3) Переход от одного блока к другому в блокчейне

4) Запись в компьютере текущих действий с блокчейном

7. Приведены примеры, как можно заработать криптовалюту. Укажите ошибочное утверждение.

1) Создание нового блока в процессе майнинга

2) Поступление криптовалюты за счет перевода с других кошельков

3) Запись произвольной суммы в свой кошелек

4) Комиссионные за включение чужих транзакций в новый блок майнером

8. Пул транзакций – это

1) Список неподтвержденных транзакций для включения в новые блоки

2) Организация группы майнеров для совместной работы

3) Исчерпывающий список пользователей блокчейна

4) Максимальное количество возможных транзакций

Разработчики:

доцент, к.ф.-м.н. В.И., Красов

(подпись) *(занимаемая должность)* *(инициалы, фамилия)*

11.3. Оценочные средства для промежуточной аттестации

Материалы для проведения текущего и промежуточного контроля знаний студентов:

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1.	Собеседование при защите готовой программы	Все темы	ПК-3
2.	Подготовка к зачету	Все разделы	ПК-3

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ОПОП по направлению и профилю подготовки **10.03.01 Информационная безопасность.**

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» марта 2020 г.

Протокол № 8 И.О.Зав. кафедрой  Колесник С.Н.