МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Основы технологии блокчейн

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью изучения дисциплины «Основы технологии блокчейн» является освоение обучающимися передовых знаний в области практической криптографии, а именно вопросов, связанных с применением блокчейн технологий для обеспечения информационной безопасности.

Дисциплина обеспечивает приобретение знаний, умений и навыков в области использования блокчейн технологий, способствует освоению принципов корректного применения современных криптографических средств и методов защиты информации.

Задачами освоения дисциплины «Основы технологии блокчейн» являются:

- приобретение знаний о блокчейн технологиях;
- приобретение умений по использованию блокчейн технологий;
- приобретение навыков разработки и проектирования блокчейн систем.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, и является дисциплиной по выбору.

Для освоения данной дисциплины обучающиеся должны знать основные криптографические понятия и методы, владеть методами программирования, уметь осуществлять программную реализацию известных алгоритмов.

Для успешного освоения дисциплины «Основы технологии блокчейн» ей должны предшествовать следующие дисциплины:

«Теоретико-числовые методы в криптографии»;
«Сложность вычислений»;
«Теория алгоритмов».

Дисциплина «Основы технологии блокчейн» является предшествующей для прохождения производственной и преддипломной практики и итоговой государственной аттестации.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		

ПК-1 Способен разрабатывать математические модели систем обеспечения информационной безопасности, математически доказывать их соответствие выбранным политикам безопасности	И-ПК-1.1 Знает основные математические модели систем обеспечения информационной безопасности и математические методы обеспечения информационной безопасности	Знать: - основные математические модели блокчейн систем; - языки программирования блокчейн систем.
	И-ПК-1.2 Владеет навыками разработки и реализации алгоритмов решения типовых профессиональных задач на языках высокого уровня	Владеть навыками: разработки и реализации приложений для блокчейн систем, в том числе умных контрактов
ПК-2 Способен анализировать математические модели систем обеспечения информационной безопасности, а также проводить тестирование средств защиты информации на соответствие этим моделям	И-ПК-2.1 Знает основные виды атак на информационную инфраструктуру и математические методы противодействия им	Знать: - основные виды атак на блокчейн системы, в том числе атаки двойного расходования, атаки 51 процента, паразитных цепочек и другие; - подходы к обеспечению консенсуа
	И-ПК-2.1 Умеет разрабатывать и применять математические методы противодействия атакам на информационные системы и инфраструктуру	Уметь: - применять методы противодействия основным видам атак на блокчейн системы; - проводить анализ защищенности блокчейн приложений

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 акад. часов.

№ п/п	**Темы (разделы) дисциплины, их содержание**	**Семестр**	**Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)**		**Формы текущего контроля успеваемости** **Форма промежуточной аттестации (по семестрам)**
			Контактная работа		

			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Криптографические основы технологии блокчейн	3	8			1		24	Задания для самостоятельной работы
2	Основы технологии блокчейн	3	4			1			
3	Технология Bitcoin	3	4			1			
4	Технология Etherium	3	4	8		1		16	Задания для самостоятельной работы
5	Разработка блокчейн приложений	3	4	8		1		16	Задания для самостоятельной работы
6	Разработка приложений Etherium	3	4	16		1		16	Задания для самостоятельной работы
7	Технология Tangle	3	4			2			
						2	0,5	33,5	Экзамен
	ИТОГО	**180**	**32**	**32**		**10**	**0,5**	**105,5**	

Содержание дисциплины «Основы технологии блокчейн»:

Тема 1. Криптографические основы технологии блокчейн.

Односторонние функции. Псевдослучайные генераторы. Псевдослучайные функции. Хэш-функции. Дерево Меркла. Электронная подпись.

Тема 2. Основы технологии блокчейн.

Что такое блокчейн. Централизованные и децентрализованные системы. Уровневая модель блокчейна. Проблема византийских генералов. Механизмы распределенного консенсуса. Свойства блокчейн решений.

Тема 3. Технология Bitcoin.

Транзакции. Структура блока. Генезис. Сеть Bitcoin. Распространение блока. Консенсус. Скрипты Bitcoin. Полные узлы и узлы-операторы. Биткойн-кошельки. Атаки на блокчейн и методы противодействия им.

Тема 4. Технология Etherium.

Структура данных. Формат счета. Концепция UTXO. Префиксное trie-дерево. Дерево Меркла-Патриции. RLP-кодирование. Транзакции и структура сообщений. Функция перехода, стоимость транзакции. Умные контракты. Типы данных в Solidity, операторы языка Solidity. Виртуальная машина и выполнение кода. Экосистема. Атаки на блокчейн и методы противодействия им.

Тема 5. Разработка блокчейн приложений.

Децентрализованные приложения. Создание блокчейн-приложений: программирование Bitcoin и Etherium приложений. Библиотека BitcoinJS: подготовка и трансляция транзакций. Взаимодействие с Etherium: настройка счетов, подготовка и трансляция транзакций. Создание и развертывание умного контакта. Вызов функции умного контракта.

Тема 6. Разработка приложений Etherium.

Настройка частной сети Etherium. Создание и развертывание умного контракта в частной сети. Библиотека web3.js. Разработка клиентского приложения для контракта.

Тема 7. Технология Tangle.

Структура данных. Транзакции и структура сообщений. Математические модели Tangle, устойчивость. Атаки на Tangle и методы противодействия им. Алгоритм MCMC.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Лекция-беседа или «диалог с аудиторией», является наиболее распространенной и сравнительно простой формой активного вовлечения студентов в учебный процесс. Эта лекция предполагает непосредственный контакт преподавателя с аудиторией. Преимущество лекции-беседы состоит в том, что она позволяет привлекать внимание студентов к наиболее

важным вопросам темы, определять содержание и темп изложения учебного материала с учетом особенностей студентов.

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала. Проблемная лекция начинается с вопросов, с постановки проблемы, которую в ходе изложения материала необходимо решить. В лекции сочетаются проблемные и информационные начала. При этом процесс познания студентов в сотрудничестве и диалоге с преподавателем приближается к поисковой, исследовательской деятельности. Содержание проблемы раскрывается путем организации поиска ее решения или суммирования и анализа традиционных и современных точек зрения.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTex;
- Adobe Acrobat Reader;

при проведении практических занятий используется программное обеспечение

- Microsoft Visual Studio.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

Для поиска учебной литературы библиотеки ЯрГУ используется автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php.

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. *Сингхал Б.* Блокчейн. Руководство для начинающих разработчиков: Пер. с англ. / Б. Сингхал, Г. Дамеджа, П. С. Панда. — СПб.: БХВ-Петербург, 2020. – 288 с.

б) дополнительная литература

1. Прасти Н. Блокчен. Разработка приложений: Пер. с англ. / Н. Прасти — СПб.: БХВ-Петербург, 2018. – 256 с.

2. Ethereum: A secure decentralized generalized transaction ledger, Version 80085f7 – 2021-07-11 (или более поздняя).

3. The Tangle, Version 1.4.2 (или более поздняя).

4. Zcash Protocol Specifcation, Version 2021.2.13 (или более поздняя).

5. Bitcoin: пиринговая электронная платежная система: Nakmoto, Sotoshi, «Bitcoin: A Peer-to-Peer Electronic Cash System», https://bitcoin.org/bitcoin.pdf

в) ресурсы сети «Интернет» (при необходимости)

https://github.com/ – веб-сервис для размещения IT-проектов и их совместной разработки.

https://bitcoin.org/ – сайт биткойн-сообщества. Содержит различные материалы по экосистеме Bitcoin, в том числе документацию для разработчиков.

https://ethereum.org/ru/ – сайт Ethereum-сообщества. Содержит различные материалы по экосистеме Bitcoin, в том числе документацию для разработчиков.

https://zkp.science/ – сайт, посвященный доказательствам с нулевым разглашением.
https://www.youtube.com/channel/UCYWsYz5cKw4wZ9Mpe4kuM_g/videos – youtube канал, посвященный доказательствам с нулевым разглашением.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения лабораторных работ, оснащенные средствами вычислительной техники, с установленным программным обеспечением Microsoft Visual Studio;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):
Доцент кафедры КБиММОИ, канд. физ.-мат. наук Д.М. Мурин

Приложение № 1 к рабочей программе дисциплины
«Основы технологии блокчейн»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Задания для самостоятельной работы

Задания для самостоятельной работы по теме № 1 «Криптографические основы технологии блокчейн»

Варианты заданий по подтеме «Односторонние функции».

Упражнение 1. Функция называется регулярной, если она принимает значения одинаковой длины на входах одинаковой длины. Докажите, что если существует односторонняя функция, то существует и регулярная односторонняя функция.

Упражнение 2. Функция называется сохраняющей длину, если она принимает значения, длина которых совпадает с длиной входов. Докажите, что если существует односторонняя функция, то существует и односторонняя функция, сохраняющая длину.

Упражнение 3. Постройте функцию, сохраняющую длину на всех длинах входов.

Упражнение 4. Изменится ли понятие «односторонняя функция», если в определении наделить нарушителя возможностью использовать детерминированную полиномиальную машину Тьюринга вместо вероятностной полиномиальной машины Тьюринга?

Упражнение 5. Изменится ли понятие «односторонняя функция», если предположить, что она (функция) является вычислимой за полиномиальное время на вероятностной машине Тьюринга, а не на детерминированной машине Тьюринга?

Упражнение 6. К каким последствиям может привести неравномерное распределение входных строк x на множестве $\{0, 1\}^n$?

Варианты заданий по подтеме «Генераторы псевдослучайных чисел».

1. Докажите, что отношение «быть вычислительно неразличимым» рефлексивно, симметрично и транзитивно.

2. Пусть α_n и β_n вычислительно неразличимы, $q(n)$ – полином, $U_{q(n)}$ - случайная величина, определенная и равномерно распределенная на битовых строках длины $q(n)$. Докажите, что $\alpha_n U_{q(n)}$ и $\beta_n U_{q(n)}$ вычислительно неразличимы.

3. Пусть α_n и β_n вычислительно неразличимы, f – полиномиально вычислимая функция. Докажите, что $f(\alpha_n)$ и $f(\beta_n)$ вычислительно неразличимы.

Варианты заданий по подтеме «Хэш-функции».

1. Используя подходящее семейство хеш-функций AXU, представьте конструкцию совершенно безопасного одноразового MAC. Кроме того, представьте такой MAC, в котором теги аутентификации имеют фиксированную длину (т. е. в зависимости от длины ключа, но не от длины аутентифицируемого сообщения).

2. Покажите, что любой совершенный безопасный одноразовый MAC, который использует теги аутентификации фиксированной длины и детерминированный алгоритм подписи, дает обобщенный ансамбль хеширования с незначительной вероятностью коллизий. В частности, для любого многочлена p этот ансамбль обладает свойством $(p, 1 / p)$-коллизии.

Варианты заданий по подтеме «Псевдослучайные функции».

1. Существует ли какой-нибудь конкретный тест, из которого следует случайность по всем остальным?

2. Постройте из псевдослучайного генератора $G : B^n \to B^N$ псевдослучайную функцию $F : n \times \log N \to \{0,1\}$.

Варианты заданий по подтеме: «Электронные подписи».

1. Доказать, что существование семейств хеш-функций без коллизий влечет существование односторонних функций.

2. Докажите, что функция Рабина $f_m(x) = x^2 \bmod m$, где $m = pq$, p, q – простые числа представимые в виде $4k + 3$ при натуральном k, задает перестановку на множестве квадратичных вычетов по модулю m.

Задания для самостоятельной работы по теме № 4 «Технология Ethereum»

Задания для самостоятельной работы по теме № 4 «Технология Ethereum»

Установка Ethereum Wallet. Цель работы: Получение представлений и начальных навыков работы в сети Ethereum. Результаты самостоятельной работы: Установленный кошелек Ethereum Mist Wallet.

Задания для самостоятельной работы по теме № 5 «Разработка блокчейн приложений»

Знакомство с инструментами и средой разработки умных контрактов. Цель работы: изучение и закрепление на практике возможностей основных инструментов разработчика умных контрактов. Результаты самостоятельной работы: Установленный кошелек MetaMask, настроенный на работу с тестовой сетью Rinkeby.

Задания для самостоятельной работы по теме № 6 «Разработка приложений Etherium»

1. Знакомство с Remix – web-средой Solidity IDE. Цель работы: изучение и закрепление на практике возможностей среды разработчика умных контрактов Remix. Результаты самостоятельной работы: Практические навыки работы с инструментами среды разработчика умных контрактов Remix.

2. Язык программирования умных контрактов Solidity. Цель работы: изучение и закрепление на практике основных синтаксических конструкций языка программирования Solidity Результаты самостоятельной работы: разработанные простые контрактов.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к экзамену:

1. Односторонние функции.
2. Псевдослучайные генераторы.
3. Псевдослучайные функции.
4. Хэш-функции. Дерево Меркла.
5. Электронная подпись.
6. Централизованные и децентрализованные системы. Уровневая модель блокчейна.
7. Проблема византийских генералов.
8. Механизмы распределенного консенсуса.
9. Технология Bitcoin. Структура транзакции и блока. Генезис. Сеть Bitcoin: полные узлы и узлы-операторы, распространение блока.
10. Атаки на блокчейн Bitcoin и методы противодействия им.
11. Технология Etherium. Структура данных. Концепция UTXO. Транзакции и структура сообщений, стоимость транзакции.
12. Префиксное trie-дерево. Дерево Меркла-Патриции. Функция перехода.
13. Умные контракты. Виртуальная машина и выполнение кода.
14. Атаки на блокчейн Etherium и методы противодействия им.
15. Технология Tangle. Структура данных. Транзакции и структура сообщений.
16. Математические модели Tangle, устойчивость Tangle.
17. Атаки на Tangle и методы противодействия им. Алгоритм MCMC.

Правила выставления оценки на экзамене.

В экзаменационный билет включается один теоретический вопрос. На подготовку к ответу дается не менее 1 академического часа.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется студенту, который успешно сдал все практические задания и самостоятельные работы и демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом блокчейн технологий; умеет связывать теорию с практикой. Студент дает развернутые, полные и четкие ответы на вопросы

экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию.

Оценка «Хорошо» выставляется студенту, который успешно сдал все практические задания и самостоятельные работы и ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется студенту, который успешно сдал все практические задания и самостоятельные работы, возможно за исключением одной из них, и дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагаются с использованием терминологии блокчейн технологий, но при этом допускаются ошибки в определениях некоторых основных понятий, формулировках положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется студенту, который не сдал более одного практического задания или самостоятельной работы, и демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении сущности раскрываемых понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение № 2 к рабочей программе дисциплины
«Основы технологии блокчейн»

Методические указания для студентов по освоению дисциплины

Учебным планом на изучение дисциплины «Основы технологии блокчейн» отводится один семестр, по завершении которого в качестве итогового контроля предусмотрен экзамен. В процессе изучения дисциплины проводятся практические занятия, выполняются четыре домашних задания.

При изучении дисциплины «Основы технологии блокчейн», используются лекции, практические и самостоятельные работы. Для успешного освоения дисциплины важно, чтобы обучающийся уделил особенное внимание выполнению практических и самостоятельных работ. Теоретические основы, необходимые для выполнения лабораторных работ, подробно разбираются на лекционных занятиях. Основная цель выполнения практических и самостоятельных работ – дать обучающимся представление о возможной практической деятельности в области разработки и применения блокчейн технологий для защиты информации. Для успешного выполнения практических и самостоятельных работ необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.

В качестве заданий для самостоятельной работы дома обучающимся предлагаются математические или практические упражнения, которые должны позволить обучающемуся лучше изучить понятия и методы, применяемые им для решения типовых задач из соответствующих разделов дисциплины. Решения задач должны быть подготовлены, оформлены и представлены в установленные сроки.

По итогам изучения дисциплины обучающиеся сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя один теоретический вопрос. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.