Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра информационных технологий и прикладной математики

ОДОБРЕНО:
Руководитель ОП
_____ Е.В. Мельникова
(подпись)
«01» 09 2022 г.

Рабочая программа дисциплины
Блокчейн

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы:	Безопасность компьютерных систем (по отраслям или в сфере профессиональной деятельности)

Иваново

1. Цели освоения дисциплины

Целью изучения дисциплины изучение особенностей технологии блокчейн и использования криптовалют, формирование навыков и умений инвестирования в криптовалюты и применения механизма ICO для финансового обеспечения инновационного проекта.

При изучении курса ставятся следующие задачи:

− Изучение теоретических основ технологии блокчейн и инвестирования в криптовалюты. − Формирование знаний о функционировании механизма ICO.

− Изучение основных типов криптовалют и особенностей их эмиссии.

− Приобретение практических навыков и умений выбора и использования криптовалют как объекта инвестирования.

− Формирование навыков и умений использования инструментария ICO для привлечения финансовых средств в инновационный проект.

В результате изучения данного курса, обучающиеся получат знания об особенностях использования технологии блокчейн, приобретут навыки и умения выбора, наиболее подходящих для инвестирования криптовалют, научатся использовать механизм ICO для привлечения финансовых средств в инновационный проект.

2. Место дисциплины в структуре ОП

Дисциплина является факультативом.

Успешное освоение данной дисциплины будет способствовать готовности студентов к прохождению преддипломной практики, выполнению выпускной квалификационной работы.

Студент, приступающий к изучению дисциплины, должен обладать знаниями, умениями, навыками/опытом практической деятельности, полученными ранее в ходе изучения дисциплин: Математический анализ, Математическая логика и теория алгоритмов, Языки программирования, Технологии разработки программного обеспечения, Правовое обеспечение профессиональной деятельности, Базы данных, Основы информационной безопасности, Экономика и управление.

Для освоения данной дисциплины обучающийся должен:

Знать:

– основные понятия экономической сферы;

– основы инвестирования;

– управление инновациями;

– основы криптографии и информационной безопасности.

Уметь:

– управлять личным временем;

– составлять план оптимизации.

Иметь:

– навыки разработки программ на языке программирования C++, Python.

3. Планируемые результаты обучения по дисциплине

3.1. Компетенции, формированию которых способствует дисциплина

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

а) универсальные (УК):

УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.

б) общепрофессиональные (ОПК):

ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности.

ОПК-7: Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности.

в) профессиональные (ПК):

ПК-1: Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и систем программирования для решения профессиональных задач.

3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

- основные понятия блокчейна (ОПК-2);
- требования, принципы построения хеш-функций (ОПК-2);
- сетевые протоколы взаимодействия (ОПК-7);
- стратегии майнинга (УК-2);
- основные криптовалюты, их свойства, историю и отличия (УК-2);
- правовые аспекты работы с блокчейном (УК-1).

Уметь:

- организовать транзакции в блоке (ПК-1);
- предотвратить кражу в открытых блокчейн-системах (ПК-1);
- блокировать переводы (ОПК-2);
- создавать смарт-контракты (ОПК-7).

Иметь:

- практический опыт создания пары ключей GPG, подписи и шифрования (ОПК-7);
- навык работы с тестнетом Ethereum (ПК-1);
- практический опыт использования Bitcoin Script (ОПК-2);
- навык написания смарт-контракта на Etherium и Tendermint (ОПК-7);
- навык работы с Hyperledger Fabric (ПК-1).

4. Объем и содержание дисциплины

Объем дисциплины составляет 1 зачетная единица (36 академических часов).

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

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

№ п/п	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в ак.часах, по очной форме обучения)		Формы текущего контроля успеваемости (по очной форме обучения) Формы промежуточной аттестации
			Занятия лекцион-ного типа	Занятия семинар-ского типа	
1.	Введение	8	1	1	Входная диагностика: тест с последующим обсуждением результатов.
2.	Сетевой уровень взаимодействия и	8	1	1	Практическая работа

	архитектура узла блокчейна				
3.	Архитектура блокчейн-протоколов	8	1	1	Практическая работа
4.	Протоколы консенсуса	8	1	1	Практическая работа
5.	Смарт-контракты	8	1	1	Практическая работа
6.	Протоколы анонимизации	8	1	1	Практическая работа
7.	Масштабирование сетей блокчейн	8	1	1	Практическая работа
8.	Пользовательские аспекты работы с блокчейном	8	1	1	Практическая работа
Итого за семестр:			8	8	Зачет
Итого по дисциплине:			8	8	

4.2. Развернутое описание содержания дисциплины по разделам (темам)

1. Введение

Основы блокчейна: свойства, состояния, транзакции, блоки. Доверие к участникам сети. Работа с GPG: создание пары ключей, подпись, шифрование. Подключение к тестнету BTC, создание кошелька, работа с эксплорером. Работа с тестнетом Ethereum. Понятие и история шифра, принцип Кирхгофа. Симметричное шифрование, шифр Вернама, поточные и блочные шифры. Хеш-функции: требования, принципы построения, примеры. Случайный оракул, подпись Лэмпорта, MAC, аутентифицированное шифрование. Защита хеш-функций и атаки на них. Шифрование с открытым ключом. Понятия группы, кольца, поля. Протокол шифрования RSA, протокол Диффи — Хеллмана, система Эль-Гамаля. Цифровые подписи, назначение и требования. Подпись ECDSA и Шнорра, протокол подписи RSA, подписи на основании хеш-функций. Представление о PKI — инфраструктуре открытых ключей. Представление о вычислениях на несколько сторон. Схема разделения секрета Шамира. Схема commit-reveal. Криптографические протоколы garbled circuits и oblivious transfer. ORAM.

2. Сетевой уровень взаимодействия и архитектура узла блокчейна

P2P-сети: примеры и отличия от архитектуры «клиент-сервер». Маршрутизация, bootstrapping P2P-клиента, announce vs request. Балансировка. Неструктурированные и структурированные оверлеи. Распределѐнные хеш-таблицы. Хранение файлов в P2P и атаки на P2P. BitTorrent. IPFS. Распространение информации в Bitcoin, разница в распространении транзакций и блоков, дополнительные relay-сети, протоколы исключения.

3. Архитектура блокчейн-протоколов

Организация транзакций в блоке, структура заголовка блока, полноценные и лѐгкие ноды, мемпул. Адреса в Bitcoin, Ethereum, Merkle tree, SegWit.

4. Протоколы консенсуса

Протокол BFT — задача о византийских генералах. Обзор протоколов Paxos и Raft, масштабирование протоколов. Протоколы Proof-of-Work, майнинг, атака 51%. Препятствия децентрализации в PoW-системах: ASIC, пулы. Меры противодействия централизации. Масштабирование и пересчѐт сложности майнинга, coin hopping. Стратегии майнинга: форки, эгоистичный майнинг, выборочное включение транзакций, объединѐнный майнинг. Проблемы PoW. Протоколы Proof-of-Stake. Атаки: nothing-at-stake, grinding attack. Пулы в PoS-системах. Другие варианты консенсуса: Delegated PoS, Proof-of-Space, Proof-of-Authority, Hashgraph.

5. Смарт-контракты

Блокчейн как абстрактный автомат. Стековая машина Bitcoin, скрипты Bitcoin и их ограничения. Bitcoin Script. Смарт-контракты Ethereum, их примеры и уязвимости. Газ в Ethereum: проблема останова, EVM. Solidity.

6. Протоколы анонимизации

Протоколы миксинга и конфиденциального вычисления. Кольцевые подписи, stealth-адреса. Концепция обязательств Педерсена, доказательства принадлежности интервалу. Анонимизация в Monero. Криптовалюты Mimblewimble и Grin. Анонимизация в Zcash и представление о zkSNARK.

7. Масштабирование сетей блокчейн

Офчейн-протоколы. Lightning. Сайдчейны. Шардинг. Предполагаемые решения Ethereum 2.0, альтернативные решения.

8. Пользовательские аспекты работы с блокчейном

Разберѐм примеры организации клиентского программного обеспечения, а также правовые основы работы с криптоактивами. Permissioned-модели открытых блокчейнов и обзор решений. Кошельки и хранение ключей. Получение ключей из сид-фразы и иерархические детерминистические кошельки. Функционирование криптобирж. Устройство и проблемы смарт-контрактов DAO, ICO, DeFi. Примеры DeFi и практика написания. Правовые аспекты работы с блокчейном

5. Образовательные технологии

Организация учебного процесса осуществляется в форме лекций, практических занятий и индивидуальной самостоятельной работы студентов.

Учебный процесс по дисциплине основан на использовании:

– интерактивных образовательных технологий;

– кейс-технологий;

– проектных технологий;

– технологий последовательно погружения обучения – основные темы курса на лекциях и лабораторных занятиях раскрываются через постановку и последующее разрешение проблемы создания алгоритма решения задачи и ее разрешение;

– технологий тестового контроля качества образования – в процессе и по завершении теоретического обучения выполняется тестирование.

В перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, входят:

– технологии смешанного обучения (ЭИОС «Мой университет»);

– мультимедиа технологии (проектор, видеоролики, презентации (Prezi, Microsoft PowerPoint, Google Презентации));

– web-квесты (OnlineTestPad);

– технологии визуализации (draw.io, Google DataStudio).

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Для дисциплины предусмотрены два вида самостоятельной работы:

1. Проработка лекционного материала в виде самостоятельной работы над практическими заданиями. Выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

2. Работа над самостоятельным проектом на основе практических работ. Выполняется студентом по заданию преподавателя, но без его непосредственного участия.

К зачету допускаются студенты, которые систематически, в течение всего семестра работали на занятиях и показали уверенные знания по вопросам, выносившимся на групповые занятия.

Непосредственная подготовка к зачету осуществляется по вопросам, представленным в приложении к РПД на основе МУ (приложение №1).

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

Предусмотрены:

- индивидуальное собеседование со студентами;
- рефераты по темам с наибольшим количеством часов для самостоятельной работы.
- зачет (программа зачетов см. ФОС).

Критерии оценки.

Большинство учебных задач прил. имеют внутреннюю логическую структуру и при выработке оценки их выполнения они могут быть разбиты на несколько относительно самостоятельных блоков, выполнение каждого из которых может быть оценено (например, в процентной форме), кроме того, каждый из блоков задачи может быть снабжен весом. Вес задачи считается равным сумме весов всех ее блоков.

Абсолютная оценка по отдельной задаче вычисляется как сумма процентных оценок по каждому из блоков, домноженных на вес соответствующего блока. Относительная оценка является процентной, она вычисляется делением абсолютной оценки на суммарный вес задачи.

Разбиение задачи на блоки и определение их весов не подлежит однозначной фиксации. Это является правом и заботой эксперта (ведущего лектора, группового преподавателя). Некоторая предварительная информация об установленных преподавателем весах задач может быть доведена до студентов.

Может быть вычислена итоговая оценка за определенный период обучения. В абсолютной форме она складывается из абсолютных оценок за каждую из решавшихся задач.

Итоговая оценка в относительной форме является процентной; она вычисляется делением итоговой абсолютной оценки на сумму весов всех задач.

На основе итоговой относительной оценки могут быть заданы уровни усвоения материала; например, четыре уровня: зачетные («отлично» - более 90% усвоенного материала, «хорошо» - более 70%, удовлетворительно - более 40%) и незачетный.

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Буликов, С. Н. Технология блокчейн в финансировании проектов: учебник-презентация : [16+] / С. Н. Буликов, А. А. Киселев, В. Д. Сухов. – Москва ; Берлин : Директ-Медиа, 2020. – 114 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=577851 (дата обращения: 01.09.2021). – Библиогр.: с. 99-101. – ISBN 978-5-4499-1307-4. – DOI 10.23681/577851. – Текст : электронный.

2. Целых, А. А. Современные технологии противодействия финансовым преступлениям : учебное пособие : [16+] / А. А. Целых, А. Н. Целых, Э. М. Котов ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 120 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=577703 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-9275-3286-5. – Текст : электронный.

Дополнительная литература:

1. Целых, А. Н. Современные методы прикладной информатики в задачах анализа данных: учебное пособие по курсу «Методы интеллектуального анализа данных» : [16+] / А. Н. Целых, А. А. Целых, Э. М. Котов ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2021. – 130 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=683920 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-9275-3783-9. – Текст : электронный.

2. Максуров, А. А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование / А. А. Максуров. – 3-е изд. – Москва : Дашков и К°, 2021. – 212 с. – (Научные издания). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=621907 (дата обращения: 01.09.2021). – ISBN 978-5-394-04756-5. – Текст : электронный

Ресурсы информационно-телекоммуникационной сети «Интернет»:

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

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» www.biblioclub.ru

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

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

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

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

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

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

Лаборатория, оснащенная лабораторным оборудованием, комплектом специализированной учебной мебели и техническими средствами обучения.

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

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: электронные пособия (презентации, электронные словари и т.п.), аудио-визуальные пособия (аудиозаписи, видеоматериалы и т.п.), печатные пособия (таблицы, плакаты, стенды, портреты, схемы и т.п.).

Основная профессиональная образовательная программа
10.03.01 Информационная безопасность
(Безопасность компьютерных систем
(по отраслям или в сфере профессиональной деятельности))

Автор(ы) рабочей программы дисциплины: *ст. преподаватель каф. ИТиПМ Сидорова А.Д.*

Программа рассмотрена и утверждена на заседании кафедры информационных технологий и прикладной математики «_____» _____ 2022 г., протокол № _____

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ Е.В. Мельникова
(подпись)

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ Е.В. Мельникова
(подпись)

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ Е.В. Мельникова
(подпись)