МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ХАБАРОВСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ХАБАРОВСКИЙ ТЕХНИКУМ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ И ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ»

\

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.16 «Введение в блокчейн технологии»

уровень образования *основное общее образование*

Форма обучения *очная*

09.02.07 Информационные системы и программирование

Хабаровск
2022 г

Рабочая программа учебной дисциплины составлена на основе Федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1547по специальности среднего профессионального образования 09.02.07 Информационные системы и программирование.

Организация-разработчик: Краевое государственное бюджетное профессиональное образовательное учреждение «Хабаровский техникум техносферной безопасности и промышленных технологий».

Составитель: Соцков Михаил Юрьевич, преподаватель краевого государственного бюджетного профессионального образовательного учреждения «Хабаровский техникум техносферной безопасности и промышленных технологий».

Рассмотрено и одобрено на заседании ПЦК «Информатика и Вычислительная техника»

Протокол № _____ от «____»_____20_____г.

Председатель ПЦК _____ (_____).

Согласовано на заседании методического совета
Протокол № _____ от «____»_____ 2022г

Председатель МС _____ (Линевич О. Г.)

СОДЕРЖАНИЕ

1. **ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**
ОП. 16 Введение в блокчейн технологии

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.16 «Введение в блокчейн технологии» является частью основной образовательной программы в соответствии с ФГОС СПО 09.02.07 Информационные системы и программирование, входящей в укрупненную группу специальностей 09.00.00 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: учебная дисциплина ОП.16 «Введение в блокчейн технологии», входит в профессиональный цикл как общепрофессиональная дисциплина и имеет межпредметную связь с учебными дисциплинами: ОП.02. Архитектура компьютерных систем, ОП.11. Компьютерные сети и профессиональными модулями ПМ. 01 Разработка модулей программного обеспечения для компьютерных систем, ПМ.02 Осуществление интеграции программных модулей, ПМ.04 Сопровождение информационных систем.

1.3. Цель и планируемые результаты освоения дисциплины:

Код ПК, ОК	Умения	Знания
ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 9, ОК 10, ПК 2.4	- управлять учетными записями, настраивать параметры рабочей среды пользователей; - управлять дисками и файловыми системами, настраивать сетевые параметры, - базовыми навыками работы на платформах Эзериум и Экзонум. - спроектировать блокчейн-приложение от формулировки прикладной задачи до технического описания; - моделировать криптографические примитивы и простейшие блокчейны - управлять разделением ресурсов в локальной сети.	- основные понятия, функции, состав и принципы работы технологии блокчейн; - архитектуры систем распределённого реестра - принципы управления эфиром; - блокчейн, таксономию блокчейнов, область их применимости и технологические ограничения, математические основы блокчейна

ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с

	учетом особенностей социального и культурного контекста.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.

Код	Наименование видов деятельности и профессиональных компетенций
ПК 2.4	Осуществлять разработку тестовых наборов и тестовых сценариев для программного обеспечения.

- личностные результаты

Личностные результаты реализации программы воспитания *(дескрипторы)*	Код личностных результатов
Осознающий себя гражданином и защитником великой страны	ЛР 1
Готовый использовать свой личный и профессиональный потенциал для защиты национальных интересов России	ЛР 2
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России	ЛР 3
Принимающий семейные ценности своего народа, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания	ЛР 4
Занимающий активную гражданскую позицию избирателя, волонтера, общественного деятеля	ЛР 5
Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение	ЛР 6
Готовый соответствовать ожиданиям работодателей: проектно мыслящий, эффективно взаимодействующий с членами команды и сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, нацеленный на достижение поставленных целей; демонстрирующий профессиональную жизнестойкость	ЛР 7
Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы; управляющий собственным профессиональным развитием; рефлексивно оценивающий собственный жизненный опыт, критерии личной успешности	ЛР 8
Уважающий этнокультурные, религиозные права человека, в том числе с особенностями развития; ценящий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности»	ЛР 9
Принимающий активное участие в социально значимых мероприятиях, соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России; готовый оказать поддержку нуждающимся	ЛР 10
Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением	ЛР 11
Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих	ЛР 12
Способный в цифровой среде использовать различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»	ЛР 13

Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве .	ЛР 16
Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению	ЛР 17
Осознающий значимость системного познания мира, критического осмысления накопленного опыта	ЛР 18
Развивающий творческие способности, способный креативно мыслить	ЛР 19
Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации	ЛР 20
Готовый к профессиональной конкуренции и конструктивной реакции на критику	ЛР 21
Самостоятельный и ответственный в принятии решений во всех сферах своей дея-тельности, готовый к исполнению разнообразных социальных ролей, востребован-ных бизнесом, обществом и государством	ЛР 23
Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики	ЛР 34

1.4. Количество часов на освоение программы дисциплины:
максимальная учебная нагрузка обучающегося 80 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 70 часов;

самостоятельной работы обучающегося 2часов.

2.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙДИСЦИПЛИНЫ
2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Объем образовательной нагрузки	**80**
Всего учебных занятий	70
в том числе:	
лекции, уроки	30
практические занятия	40
Самостоятельная работа	**2ч**
Консультации	2ч
Экзамен	
Форма промежуточной аттестации –экзамен	*6 семестр*

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Уровень освоения	Осваиваемые элементы компетенций
Тема 1. Введение в блокчейн.	Система распределённого реестра. История блокчейна, определение, развитие и основные продукты, примеры индустриального применения. Основы блокчейна: свойства, состояния, транзакции, блоки. Доверие к участникам сети. Блокчейн как технология в основе Биткоина. Таксономия блокчейнов. Препарируя Биткоин: сетевой протокол и клиенты.	**6**	**2**	ОК 1-5 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
	Практика: Работа с GPG: создание пары ключей, подпись, шифрование. Подключение к тестнету BTC, создание кошелька, работа с эксплорером. Работа с тестнетомEthereum. Моя игрушечная криптовалюта (практика).	**6**	**3**	
Тема 2. Криптографические основы блокчейна.	Понятие и история шифра, принцип Кирхгофа. Симметричное шифрование, шифр Вернама, поточные и блочные шифр. Хэш-функции: требования, принципы построения, примеры. Случайный оракул, подпись Лэмпорта, MAC, аутентифицированное шифрование. Защита хэш-функции 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 хэш-функций. Представление о PKI — инфраструктуре открытых ключей. Представление о вычислениях на несколько сторон. Схема разделения секрета Шамира. Схема commit-reveal. Криптографические протоколы garbledcircuits и obliviousttransfer. ORAM.	**4**	**2**	ОК 1-5 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
	Практика:Использование криптографических утилит.	**2**	**3**	
Тема 3. Архитектура узла сети блокчейн.	Верхнеуровневая архитектура узла сети блокчейн, принципы построения и взаимодействия подсистем.Организация транзакций в блоке, структура заголовка блока, лёгкие ноды.Адреса в Bitcoin и Ethereum.MerkleTree.SegWit.	**4**	**2**	ОК 1-5 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
	Практика:Реализация архитектуры узла.	**2**	**3**	

Тема 4. Сетевой уровень взаимодействия.	Организация P2P-взаимодействия. Сетьблокчейн —сеть без выделенного центра, отличия от архитектуры «клиент-сервер».P2P-сети: история, примеры, отличия от client-server. Проблемыадресации, bootstrappingP2P-клиента, announcevsrequest. Распространение информации в сети bitcoin, разница в распространении транзакций и блоков, дополнительные relay-сети, протоколы исключения некорректно работающих узлов.	**6**	**2**	ОК 1-5 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
	Практика:Написание простейшей P2P-сети.	**6**	**3**	
Тема 5. Протоколы консенсуса.	Вопросы безопасности. 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 пересчёт сложности майнинга, coinhopping. Стратегии майнинга: форки, эгоистичный майнинг, выборочное включение транзакций, объединённый майнинг. ПроблемыPoW. Протоколы Proof-of-Stake. Атаки: nothing-at-stake, grinding attack. ПулывPoS-системах. Другиевариантыконсенсуса: Delegated PoS, Proof-of-Space, Proof-of-Authority, Hashgraph.	**4**	**2**	ОК 1-5 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
Тема 6. Умные контракты.	Блокчейн как абстрактный автомат. Стековая машина bitcoin, скрипты bitcoin и их ограничения. Смарт-контракты Ethereum, их примеры и уязвимости. Газ в сети Ethereum: проблема останова, EVM. Solidity.	**4**	**2**	ОК 1-5 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
	Практика: BitcoinScript Написание смарт-контрактов Ethereum Написание смарт-контрактов Tendermint	**8**	**3**	
Тема 7. Протоколы анонимизации.	Скрытие общеизвестных деталей транзакций, но при этом предоставление доказательства их корректности. Протоколы миксинга и конфиденциального вычисления. Кольцевые подписи, stealth-адреса, mix-in. Концепция обязательств Педерсена, доказательства принадлежности интервалу. Анонимизация в Monero. Криптовалюты Mimblewimble и Grin. Анонимизация в ZCash и представление о zk-SNARK.	**2**	**2**	ОК 1-5 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23

Тема 8. Закрытые блокчейны и системы с разрешением.	Закрытые блокчейны отличия от открытых, в каких случаях они полезны.	**2**	**2**	ОК 1-5, ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
	Практика: работа с HyperledgerFabric.	**4**	**3**	
Тема 9. Масштабирование сетей блокчейн	Проблемы масштабирования на большое число клиентов. Оффчейн-протоколы. Lightning. Сайдчейны. Шардинг. Предполагаемые решения Ethereum 2.0, альтернативные решения.	**2**	**2**	ОК 1-5 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
	Практика:Применение на практике методов и способов масштабирования	**2**	**3**	
Тема 10. Пользовательские аспекты работы с блокчейном	Примеры организации клиентского программного обеспечения, а также правовые основы работы с криптоактивами. Правовые аспекты работы с блокчейном Кошельки и хранение ключей. Получение ключей из сид-фразы и иерархические детерминистские кошельки. Функционирование криптобирж. Устройство и проблемы смарт-контрактов, DAO, ICO, DeFi Направления развития блокчейна,Международная криптовалютная биржа Binance	**2**	**2**	ОК 1-5 ОК 9, 10 ПК 2.4 ЛР 1-12 ЛР 13, 16-23
	Практика: Примеры DeFi и практика написания.	**6**	**3**	
Самостоятельная работа		**2**	**3**	
Итого		**72**		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-техническое обеспечение

Реализация программы предполагает наличие лаборатории «Вычислительной техники, архитектуры персонального компьютера и периферийных устройств».

Оборудование лаборатории и рабочих мест лаборатории:

Автоматизированные рабочие места на 12обучающихся (Процессор не ниже Core13, оперативная память объемом не менее 4 Гб;) или аналоги;

Автоматизированное рабочее место преподавателя (Процессор не ниже Corei3, оперативная память объемом не менее 4 Гб;) или аналоги;

12 комплектов компьютерных комплектующих для произведения сборки, разборки и сервисного обслуживания ПК и оргтехники;

Специализированная мебель для сервисного обслуживания ПК с заземлением и защитой от статического напряжения;

Проектор и экран;

Маркерная доска;

Программное обеспечение общего и профессионального назначения:

- Для успешного освоения дисциплины, студент использует следующие программные средства:
- Веб-приложение Jupyternotebook с базовым набором библиотек языка Python: numpy, matplotlib,socket.Клиент высокоуровневого языка для виртуальной машины Ethereum под названием Solidity, например, Geth, AlethZero или ихвеб-аналоги.
- КомпиляторRust.
- КомпиляторJava.

3.2. Информационное обеспечение обучения

Перечень используемых учебных изданий. Интернет-ресурсов, дополнительной литературы:

1. Swan M. Blockchain: Blueprint for a new economy. – " O'Reilly Media, Inc.",2015.
2. Katz J. et al. Handbook of applied cryptography. – CRC press,2016.
3. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. –2018.
4. Wood G. Ethereum: A secure decentralisedgeneralised transaction ledger //Ethereum project yel- low paper. – 2016. – Vol. 151. – P. 1-32.
5. Sasson E. B. et al. Zerocash: Decentralized anonymous payments from bitcoin //Security and Priva- cy (SP), 2016 IEEE Symposium on. – IEEE, 2014. – P.459-474.
6. Yanovich Y., Mischenko P., Ostrovskiy A. Shared send untangling in bitcoin. – Working Paper, Bitfury Group Limited,2016.

7. Prihodko P. et al. Flare: An approach to routing in lightning network //White Paper –2016.

8. Ermilov D., Panov M., Yanovich Y. Automatic bitcoin address clustering //Machine Learning and Applications (ICMLA), 2017 16th IEEE International Conference on. – IEEE, 2017. – P.461-466.

9. Cachin C. Architecture of the Hyperledger blockchain fabric //Workshop on Distributed Cryptocur- rencies and Consensus Ledgers. –2016.

10. https://blockgeeks.com/guides/what-is-blockchain-technology/

11. https://bitcoin.org

12. https://github.com/bitcoin/bitcoin

13. https://ethereum.org/

14. https://github.com/ethereum/

15. https://exonum.com/

16. https://github.com/exonum

4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: • основные понятия, функции, состав и принципы работы операционных систем; • архитектуры современных операционных систем; • особенности построения и функционирования семейств операционных систем "Unix" и "Windows"; • принципы управления ресурсами в операционной системе; • основные задачи администрирования и способы их выполнения в изучаемых операционные системах;	Полнота ответов, точность формулировок, не менее 70% правильных ответов. Не менее 75% правильных ответов. Актуальность темы, Адекватность результатов 11оставленным целям, полнота ответов, точность формулировок, адекватность применения профессиональной терминологии	Текущий контроль: - экспертная оценка результатов деятельности студентов при защите практических занятий и лабораторных работ, - оценка результатов внеаудиторной (самостоятельной) работы (докладов, рефератов, теоретической части проектов, учебных исследований и т.д.) - экспертная оценка результатов тестирования, контрольных работ и др. видов текущего контроля Промежуточная аттестация: в форме экзамена
Умения: • управлять параметрами загрузки операционной системы; • выполнять конфигурирование аппаратных устройств; •управлять учетными записями, настраивать параметры рабочей среды пользователей; • управлять дисками и файловыми системами, • настраивать сетевые параметры		