Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям
_____ О.Н.Здрок
«___» _____ 2020 г.

Регистрационный № УД-_____ /уч.

ТЕХНОЛОГИЯ БЛОК-ЧЕЙНА

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-31 80 09 Прикладная математика и информатика

Профилизация: Интеллектуальные системы

2020 г.

Учебная программа составлена на основе ОСВО 1-31 80 09-2019 и учебного плана G31-128/уч. от 11.04.2019 г.

СОСТАВИТЕЛИ:
С.Е. Гутников – старший преподаватель кафедры информационных систем управления факультета прикладной математики и информатики Белорусского государственного университета

РЕЦЕНЗЕНТЫ: .
А.А. Дудкин – доктор технических наук, профессор заведующий лабораторией идентификации систем ОИПИ НАН Беларуси.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой информационных систем управления
(протокол № 9 от 20 марта 2020 года);

Научно-методическим Советом БГУ

(протокол № 4 от 25 марта 2020 года).

Заведующий кафедрой
информационных систем управления _____ В.В. Краснопрошин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Учебная дисциплина «Технология блок-чейна» знакомит студентов магистратуры с фундаментальными методами и алгоритмами лежащими в основе технологии блокчейна, а также с техническими и программными концепциями, знание которых необходимо для анализа тенденций развития и разработки вариантов использования блокчейна.

Цель учебной дисциплины – развитие у студентов магистратуры навыков обработки и анализа данных с использованием технологии блок-чейна.

Задачи учебной дисциплины:

1. Создание базы для использования современных технологий обработки данных основанных на технологии блокчейна.
2. Формирование навыков применения технологии блокчейна в типовых случаях.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием (магистра).

Учебная дисциплина относится **к модулю** «Методы анализа данных» компонента учреждения высшего образования.

Программа составлена с учетом **межпредметных связей** с учебными дисциплинами. Основой для изучения учебной дисциплины являются следующие учебные дисциплины первой ступени высшего образования: «Теория вероятностей и математическая статистика», «Геометрия и алгебра», «Программирование».

Требования к компетенциям

Освоение учебной дисциплины «Технология блок-чейна» должно обеспечить формирование следующих **специализированных** компетенций:

СК–14. Уметь определять общие формы и закономерностей предметной области

СК–22. Анализировать основные тенденции развития технологии блокчейна и потенциальные сферы ее применения

В результате изучения дисциплины студент магистратуры должен:

знать:

- основные понятия из математики, криптографии и теории игр, лежащих в основе технологии блокчейна;
- методы и алгоритмы, использованные при построении самых известных блокчейнов в мире — Bitcoin и Ethereum;
- экономические основы технологии блокчейна и её место в цифровой экономике;

уметь:

- строить математические модели для решения типовых классов прикладных задач;

- проектировать блокчейн-приложения на платформах Bitcoin и Ethereum;

владеть:

- основными методами и алгоритмами обработки данных для построения приложений блокчейна в различных областях;
- навыками компьютерной реализации блокчейн-приложений.

Структура учебной дисциплины

Дисциплина изучается во 2 семестре. Всего на изучение учебной дисциплины «Технология блок-чейна» отведено:

– для очной формы получения высшего образования — 120 часов, в том числе 60 аудиторных часов, из них: лекции – 20 часов, практические занятия – 20 часов, семинарские занятия – 20 часов в дистанционной форме обучения (ДО).

Трудоемкость учебной дисциплины составляет 3 зачетных единиц.

Форма текущей аттестации по учебной дисциплине – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1 Введение в технологию блокчейн

Тема 1.1. Происхождение технологии блокчейна и её место в цифровой экономике

Понятие цифровой экономики. Экономические основы блокчейна. Преимущества и проблемы блокчейна. Криптовалюты. Правовое регулирование криптовалют. Перспективы и риски применения криптовалют.

Тема 1.2. Криптография в блокчейн-технологиях

Общие принципы работы криптографии. Принцип Керкгоффса и функция XOR. Алгоритм обмена ключами Диффи — Хеллмана.

Тема 1.3. Криптография с симметричным ключом

Потоковое и блочное шифрование. Одноразовый блокнот. Стандарт шифрования DES. Стандарт шифрования AES. Расширение ключа AES. Проблемы криптографии с симметричным ключом..

Тема 1.4. Криптография с асимметричным ключом

Алгоритм RSA. Алгоритм цифровой подписи DSA. Криптография на эллиптических кривых. Алгоритм ECDSA.

Тема 1.5. Криптографические хэш-функции

Обзор хэш-функций. SHA-2. SHA-256 и SHA-512. RIPEMD. SHA-3. Применение хэш-функций. MAC и HMAC.

Тема 1.6. Концепции информатики и теории игр в блокчейне

Равновесие по Нэшу. Дилемма заключенного. Проблема византийских генералов. Игры с нулевой суммой. Хэш-указатель. Дерево Меркла.

Тема 1.7. Свойства систем построенных на блокчейне

Транзакции в блокчейн. Механизмы распределенного консенсуса. Масштабирование и шардинг.

Раздел 2. Блокчейн-приложения

Тема 2.1. Платформа и криптовалюта Bitcoin

Назначение и терминология Bitcoin. Архитектура платформы Bitcoin. Механизмы функционирования Bitcoin. Пример использования Bitcoin.

Тема 2.2. Платформа и криптовалюта Ethereum

Назначение и терминология Ethereum. Архитектура платформы Ethereum. Механизмы функционирования Ethereum. Пример использования Ethereum.

Тема 2.3. Разработка блокчейн-приложений

Децентрализованные приложения. Создание блокчейн-приложений. Программирование приложений Bitcoin и Ethereum. Библиотеки и инструменты. Взаимодействие с блокчейном Bitcoin. Программное

взаимодействие с Ethereum. Настройка частной сети Ethereum. Создание и развертывание смарт-контракта Ethereum. Обращение к смарт-контракту Ethereum. Клиентское веб-приложение Ethereum..

Тема 2.4. Возможные области применения блокчейна

Публичные и частные блокчейны. Блокчейн в образовании, медицине, юриспруденции, документообороте, земельном кадастре. Перспективы на будущее.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования

№ п/п	Название раздела, темы	Количество аудиторных часов				Количество часов УСР	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия	Иное		
1	**Введение в технологию блокчейна**	**13**	**8**	**6**			Устный опрос.
1.1	Происхождение технологии блокчейна и её место в цифровой экономике	2					Устный опрос. Доклад.
1.2	Криптография в блокчейн-технологиях	1					Устный опрос. Доклад.
1.3	Криптография с симметричным ключом	2	2(ДО)	2			Устный опрос. Доклад. Отчеты по домашним практическим заданиям с их устной защитой.
1.4	Криптография с асимметричным ключом	2	2(ДО)	2			Устный опрос. Доклад. Отчеты по домашним практическим заданиям с их устной защитой.
1.5	Криптографические хэш-функции	2	2(ДО)	2			Устный опрос.
1.6	Концепции информатики и теории игр в блокчейне	2	2(ДО)				
1.7	Свойства систем построенных на блокчейне	2					Устный опрос. Доклад
2	**Блокчейн-приложения**	**7**	**12**	**14**			Устный опрос. Доклад
2.1	Платформа и криптовалюта Bitcoin	2	2(ДО)	4			Устный опрос. Доклад. Отчеты по домашним практическим заданиям с их устной защитой.
2.2	Платформа и криптовалюта Ethereum	2	4(ДО)	4			Устный опрос. Доклад
2.3	Разработка блокчейн-приложений	2	6(ДО)	6			Устный опрос. Доклад
2.4	Возможные области применения блокчейна	1					Устный опрос.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Сингхал, Б., Блокчейн. Руководство для начинающих разработчиков: Пер. с англ. / Б. Сингхал, Г. Дамеджа, П. С. Панда. —СПб.: БХВ-Петербург, 2019. —288 с., ISBN 978-5-9775-4052-0
2. Прасти Н., Блокчейн. Разработка приложений: Пер. с англ. — СПб.: БХВ-Петербург, 2018.—256 с., ISBN 978-5-9775-3976-0
3. Дрешер Д., Основы блокчейна: вводный курс для начинающих в 25 небольших главах / пер. с англ. А.В.Снастина. - М.: ДМК Пресс, 2018. - 312 с., ISBN 978-5-97060-591-2
4. Головенчик, Г. Г., Цифровая экономика [Электронный ресурс]: учеб.-метод. комплекс / Г. Г. Головенчик. –Минск: БГУ, 2020, ISBN 978-985-566-847-4

Перечень дополнительной литературы

1. Антонопулос А.М., Осваиваем биткойн: Пер. с англ. — М.: ДМК Пресс, 2018. - 428 с., ISBN 978-5-94074-965-3
2. Табернакулов А., Блокчейн на практике / Александр Табернакулов, Ян Койфманн. — М.: Альпина Паблишер, 2019. — 260 с., ISBN 978-5-9614-2382-2

Перечень рекомендуемых средств диагностики и методика формирования итоговой оценки

Для диагностики компетенции в рамках учебной дисциплины рекомендуется использовать следующие формы:

1. Устная форма: устный опрос, коллоквиум, выступление с докладом на семинаре.
2. Устно-письменная форма: отчеты по домашним практическим заданиям с их устной защитой, оценивание на основе проектного метода.

Формой текущей аттестации по дисциплине «Технология блок-чейна» учебным планом предусмотрен – экзамен во 2 семестре.

При формировании итоговой оценки используется рейтинговая оценка знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний в рейтинговую оценку (формирование оценки за текущую успеваемость):

- отчёты по практическим домашним заданиям с их устной защитой – 40 %;
- устный опрос – 20%;
- выступление с докладом – 40%.

Рейтинговая оценка по дисциплине рассчитывается на основе оценки текущей успеваемости и экзаменационной оценки с учетом их весовых коэффициентов Вес оценки по текущей успеваемости составляет 40 %, экзаменационная оценка – 60 %.

Примерная тематика практических занятий

Занятие № 1. Взаимодействие с блокчейном Bitcoin

Занятие № 2. Транзакции в Bitcoin, получение тестовых биткойнов

Занятие № 3. Взаимодействие с блокчейном Ethereum.

Занятие № 4. Транзакции в Ethereum.

Занятие № 5. Смарт-контракты Ethereum, развёртывание в частной сети

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса большинства практических занятий используется *практико-ориентированный подход*, который предполагает освоение содержания учебного материала через решение практических задач, а также приобретение навыков эффективного выполнения разных видов профессиональной деятельности.

Кроме этого, при организации образовательного процесса используется комбинация *методов группового обучения*, *проектного обучения* и *учебной дискуссии*. Комбинация методов предполагает: ориентацию на генерирование идей, приобретение навыков для решения исследовательских, творческих и коммуникационных задач, появление нового уровня понимания изучаемой темы, применение знаний (теорий, концепций) при решении проблем, определение способов их решения.

Методические рекомендации по организации самостоятельной работы обучающихся, подготовка к экзамену

Для организации самостоятельной работы студентов магистратуры по учебной дисциплине следует использовать современные информационные технологии: образовательный портал InsightRunner (https://acm.bsu.by), разместить в сетевом доступе комплекс учебных и учебно-методических материалов (учебно-программные материалы, учебное издание для теоретического изучения дисциплины, презентации лекций, методические указания к практическим занятиям, электронные версии домашних заданий, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации, в том числе вопросы для подготовки к зачёту, задания, вопросы для самоконтроля, список рекомендуемой литературы, информационных ресурсов и др.).

Примерный перечень вопросов к экзамену

1. Экономические основы блокчейна; преимущества и проблемы блокчейна
2. Криптовалюты; правовое регулирование криптовалют
3. Криптография с симметричным ключом

4. Одноразовый блокнот
5. Стандарт шифрования DES
6. Стандарт шифрования AES; расширение ключа AES
7. Алгоритм RSA
8. Алгоритм цифровой подписи DSA
9. Криптография на эллиптических кривых
10. Алгоритм ECDSA
11. Хэш-функции SHA-2
12. Хэш-функции SHA-256 и SHA-512
13. Хэш-функции RIPEMD
14. Хэш-функции SHA-3
15. MAC и HMAC
16. Алгоритм обмена ключами Диффи — Хеллмана
17. Равновесие по Нэшу
18. Дилемма заключенного
19. Проблема византийских генералов
20. Игры с нулевой суммой
21. Хэш-указатель
22. Дерево Меркла
23. Свойства систем построенных на блокчейне
24. Транзакции в блокчейне
25. Механизмы распределенного консенсуса
26. Масштабирование и шардинг
27. Блокчейн в формате Bitcoin
28. Дерево Меркла в Bitcoin
29. Сеть Bitcoin
30. Транзакции в Bitcoin
31. Консенсус и майнинг блоков Bitcoin
32. Блокчейн в формате Ethereum
33. Дерево Меркла-Патриции в Ethereum
34. Транзакции в Ethereum
35. Смарт-контракты Ethereum

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Интеллектуальные системы мониторинга	Информационных систем управления	Нет	Оставить содержание учебной дисциплины без изменения, (протокол № 9 от 20 марта 2020 г.)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ

на _____/_____ учебный год

№№ Пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры информационных систем управления (протокол № ____ от _____ 20__ г.)

Заведующий кафедрой
Д.т.н., профессор _____ В.В.Краснопрошин
(ученая степень, звание) (подпись) (И.О. Фамилия)

УТВЕРЖДАЮ
Декан факультета
Д.т.н., доцент _____ А.М. Недзведзь
(ученая степень, звание) (подпись) (И.О.Фамилия)