

УТВЕРЖДАЮ

Проректор по учебной работе
и образовательным инновациям



О.Н.Здрок

«30» августа 2020 г.

Регистрационный № УД- 8976 уч.

Криптотехнологии

**Учебная программа учреждения высшего образования по учебной
дисциплине для специальности:
1-31 80 03 Математика и компьютерные науки**

Профилизация: Веб-программирование и интернет-технологии

2020 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-31 80 03-2019 и учебных планов: G31-033/уч. и G31з-034/уч. от 11.04.2019

СОСТАВИТЕЛЬ:

А.Х. Перез Чернов, доцент кафедры веб-технологий и компьютерного моделирования механико-математического факультета Белорусского государственного университета, кандидат физико-математических наук.

РЕЦЕНЗЕНТ: В.Н. Мухаметов, доцент кафедры микропроцессорных систем и сетей Белорусского государственного университета информатики и радиоэлектроники, кандидат технических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой веб-технологий и компьютерного моделирования БГУ
(протокол № 9 от 20.05.2020);

Научно-методическим советом Белорусского государственного университета
(протокол № 5 от 17.06.2020).

Зав. кафедрой веб-технологий и компьютерного
моделирования, доктор физ.-мат. наук



В.М. Волков

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Целью дисциплины «Криптотехнологии» является создание у магистрантов базы для широкого использования современных распределенных технологий при разработке информационных сервисов и систем с проблемой управления доверием.

Задачи учебной дисциплины:

- расширение кругозора студентов в области их будущей профессиональной деятельности, знакомство с современными принципами и тенденциями при развертывании распределенных приложений, в том числе на основе технологий распределенного реестра и умных контрактов;
- изучение ключевых технологий и продуктов в области криптоиндустрии;
- изучение принципов согласования бизнес, социально-инженерных, экономических и технических задач при развертывании информационных систем на основе технологий распределенного реестра.

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

Учебная дисциплина является дисциплиной компонента учреждения высшего образования и входит в состав модуля «Распределенные приложения и криптотехнологии». Её преподавание тесно связано с дисциплиной «Архитектура распределенных приложений».

Требования к компетенциям

Освоение учебной дисциплины «Криптотехнологии» должно обеспечить формирование следующей **специализированной компетенции**:

СК-4. Быть способным применять ключевые методы проектирования и защиты информационных систем для реализации устойчивых распределенных систем и криптоприложений.

В результате изучения учебной дисциплины студент должен:

знать:

- основные понятия распределенных приложений и умных контрактов;
- современные тенденции и направления развития криптотехнологий;
- популярные архитектуры и проекты в области криптотехнологий;

уметь:

- проектировать и развертывать архитектуру распределенных приложений на технологиях умных контрактов и распределенного реестра;
- анализировать основные юридические, экономические, технологические и риски безопасности при разработке и развертывании криптопроектов.

владеть:

навыками практического использования современных технологий по проектированию и развертыванию приложений на основе криптотехнологий.

Структура учебной дисциплины

Форма получения высшего образования очная (дневная) и заочная.

Дисциплина изучается в 3 семестре очной и заочной формы обучения.

Всего на изучение учебной дисциплины отведено:

– для очной формы получения высшего образования – 198 часов, в том числе 70 аудиторных часа, из них: лекции – 36 часа, лабораторные занятия – 34 часов.

– для заочной формы получения высшего образования – 198 часов, в том числе 16 аудиторных часов, из них 8 часов лекции, 8 часов лабораторные занятия.

Трудоемкость учебной дисциплины составляет 6 зачетных единиц.

Формой текущей аттестации по учебной дисциплине является экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Ключевые понятия блокчейн технологий. Понятия распределенного реестра, майнинга, умного контракта, гибридных и распределенных приложений. Обзор типовых алгоритмов и архитектур в рамках криптотехнологий.

Тема 2. Сравнения архитектур реализации реестров и способов ускорения транзакций. Сравнение архитектурных подходов различных способов организации консенсуса и ускорения транзакций.

Тема 3. Правовое регулирование криптотехнологий. Правовое регулирование криптотехнологий и криптоэкономики в разных странах. Учет права при реализации проектов с участием организаций и граждан из разных стран. Процедуры KYC, тест на различие между продуктовыми и инвестиционными токенами.

Тема 4. Эмиссия токенов. Особенности эмиссии и организации ICO, оценка инвестиционной привлекательности крипто проекта, особенности рейтингования проектов, примеры изменения стоимости криптовалют в зависимости от фундаментальных и социальных параметров.

Тема 5. Умные контракты. Умные контракты и ключевые принципы их разработки, тестирование и аудит умных контрактов, построение распределенных организаций. Проблемы интеграции умных контрактов в реальные бизнес-процессы.

Тема 6. Безопасность. Типовые инфраструктурные и социальные атаки в рамках криптопроектов. Обзор рисков и сценариев. Обзор существующих перспективных проектов. Криптовиржи с позиции владельца проекта.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Литература	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	Ключевые понятия блокчейн технологий	6			6		[1, 2]	Опрос, защита творческих заданий
2	Сравнения архитектур реализации респондов и способов ускорения транзакций	6			6		[1, 2]	Опрос, тестирование
3	Правовое регулирование криптотехнологий	6			6		[1, 2]	Опрос, тестирование
4	Эмиссия токенов	6			6		[1, 2]	Опрос, тестирование
5	Умные контракты	6			6		[1, 2]	Опрос, отчет по лабораторной работе, защита творческих заданий
6	Безопасность	6			4		[1, 2]	Отчет по лабораторной работе, защита творческих заданий
	ВСЕГО	36			34			Экзамен

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Заочная форма получения образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Литература	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	Ключевые понятия блокчейн технологий	1			2		[1, 2]	Опрос, защита творческих заданий
2	Сравнения архитектур реализации рестров и способов ускорения транзакций	1			2		[1, 2]	Опрос, тестирование
3	Правовое регулирование криптотехнологий	1					[1, 2]	Опрос, тестирование
4	Эмиссия токенов	1					[1, 3]	Опрос, тестирование
5	Умные контракты	2			4		[1, 2]	Опрос, отчет по лабораторной работе, защита творческих заданий
6	Безопасность	2					[1, 2]	Отчет по лабораторной работе, защита творческих заданий
	ВСЕГО	8			8			Экзамен

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Bitcoin and Cryptocurrency Technologies [Электронный ресурс] – Электронные данные. – Режим доступа: <http://bitcoinbook.cs.princeton.edu>
2. Mastering ethereum, [Электронный ресурс] – Электронные данные. – Режим доступа: <https://github.com/ethereumbook/ethereumbook>
3. Chris Berg et al, Understanding the Blockchain Economy. An introduction to Institutional Cryptoeconomics // RMIT University, 2019

Дополнительная литература

4. IPFS [Электронный ресурс] – Электронные данные. – Режим доступа: <https://docs.ipfs.io/>
5. BigchainDB [Электронный ресурс] – Электронные данные. – Режим доступа: <https://github.com/bigchaindb/>
6. Cryptoeconomics [Электронный ресурс] – Электронные данные. – Режим доступа: <https://github.com/jpantunes/awesome-cryptoeconomics>
7. Openzeppelin [Электронный ресурс] – Электронные данные. – Режим доступа: <https://github.com/OpenZeppelin/openzeppelin-contracts>
8. Ethereum tutorial [Электронный ресурс] – Электронные данные. – Режим доступа: <https://github.com/facuspagnuolo/ethereum-spiking>
9. Новости криптотехнологий, Forklog [Электронный ресурс] – Электронные данные. – Режим доступа: <https://forklog.com>

Перечень рекомендуемых средств диагностики и методика формирования итоговой оценки

Контроль работы учащихся проходит в форме опроса на лекциях, а также во время устной защиты отчета по лабораторным работам и практическим заданиям. Оценка за ответы на лекциях и лабораторных занятиях включает в себя полноту ответа, наличие аргументации, глубину понимания. При защите лабораторных работ ценится самостоятельность выполнения, умение критически оценивать полученные результаты.

Формой текущей аттестации по дисциплине учебным планом предусмотрен экзамен. Экзамен по дисциплине проходит в устной форме.

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

Формирование оценки за текущую успеваемость:

- отчеты по лабораторным работам – 60 %;
- выполнение творческих заданий и результаты опроса на лекциях – 40 %.

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

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется *эвристический подход*, который предполагает демонстрацию многообразия решений большинства практических задач, среди которых необходимо выбрать наиболее рациональный подход. Например, стоит ли использовать возможности систем нечеткого логического вывода для аппроксимации экспериментальных данных и т.п.

При организации образовательного процесса используется **практико-ориентированный подход**, который предполагает освоение компьютерных приложений посредством изучения типичных примеров их использования и выработки навыков адаптации типовых примеров к решению других аналогичных и более сложных задач.

При организации образовательного процесса используются **методы и приемы развития критического мышления**, которые предполагают оценку не только корректности полученного решения, но и рациональность подхода, использованного при этом.

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов по учебной дисциплине рекомендованы электронные ресурсы в списке дополнительной литературы. Самостоятельное задание включает разработки возможной экономической и технической трансформации выбранной предметной области с помощью умных контрактов, эмиссии токенов, распределенных приложений: семья, отель, квартал, парковка, кафе, университет, больница, художественная галерея, торговый центр, общественный транспорт, школа.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название 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)
Архитектура распределенных приложений	Веб-технологий и компьютерного моделирования	Нет	Оставить содержание учебной программы без изменения (протокол № 9 от 20.05.2020)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
на _____ / _____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры Веб-технологий и компьютерного моделирования (протокол № __ от _____ 20 г.)

Заведующий кафедрой

доктор физ.-мат. наук
(ученая степень, ученое звание)

_____ (подпись)

В.М. Волков
(И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

доктор физ.-мат. наук
(ученая степень, ученое звание)

_____ (подпись)

С.М. Босяков
(И.О.Фамилия)