

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
Московский государственный университет имени М.В. Ломоносова  
Факультет вычислительной математики и кибернетики

**УТВЕРЖДАЮ**  
**декан факультета вычислительной**  
**математики и кибернетики**

  
**И.А. Соколов /**  
**«27» сентября 2023г.**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

**по дисциплине**

**Технология блокчейн**

---

**Уровень высшего образования:**

**бакалавриат**

**Направление подготовки / специальность:**

**02.03.02 "Фундаментальная информатика и информационные технологии" (3++)**

**Направленность (профиль) ОПОП:**

**Искусственный интеллект и анализ данных**

**Форма обучения:**

**очная**

Рассмотрен и утвержден

*на заседании Ученого совета факультета ВМК*

*(протокол №7, от 27 сентября 2023 года)*

Москва 2023

# 1. ФОРМЫ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

В процессе и по завершении изучения дисциплины оценивается формирование у студентов следующих компетенций:

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	Индикатор (показатель) достижения компетенции	Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций
ПК-5. Способен использовать инструментальные средства для решения задач машинного обучения	<p>ПК-5.1. Осуществляет оценку и выбор инструментальных средств для решения поставленной задачи</p> <p>ПК-5.2. Разрабатывает модели машинного обучения для решения задач</p> <p>ПК-5.3. Создает, поддерживает и использует системы искусственного интеллекта, включающие разработанные модели и методы, с применением выбранных инструментов машинного обучения</p>	<p>ПК-5.1. 3-1. Знает возможности современных инструментальных средств и систем программирования для решения задач анализа данных и машинного обучения</p> <p>ПК-5.1. У-1. Умеет проводить сравнительный анализ и осуществлять выбор инструментальных средств для решения задач машинного обучения</p> <p>ПК-5.2.3-1. Знает функциональные возможности современных инструментальных средств и систем программирования в области создания моделей и методов машинного обучения</p> <p>ПК-5.2. 3-2. Знает принципы проведения машинного эксперимента, проблемы переобучения и недообучения модели, требования к обучающей, тестовой и валидационной выборкам для решения задач анализа данных и машинного обучения</p> <p>ПК-5.2. У-1. Умеет применять современные инструментальные средства и системы программирования для разработки моделей машинного обучения</p> <p>ПК-5.2. У-2. Умеет планировать и выполнять машинные эксперименты, оценивать точность и качество построенных моделей</p> <p>ПК-5.3. 3-1. Знает принципы</p>

		<p>построения систем искусственного интеллекта, методы и подходы к планированию и реализации проектов по созданию систем искусственного интеллекта с применением машинного обучения</p> <p>ПК-5.3. 3-2. Знает методологию проведения массово параллельных вычислений для ускорения машинного обучения (с использованием GPU)</p> <p>ПК-5.3. 3-3. Знает принципы работы распределенных кластерных систем</p> <p>ПК-5.3. У-1. Умеет решать задачи по выполнению коллективной проектной деятельности для создания, поддержки и использования системы искусственного интеллекта с применением машинного обучения и массово параллельных вычислений для ускорения машинного обучения</p> <p>ПК-5.3. У-2. Умеет работать с распределенной кластерной системой при создании, поддержке и использовании систем искусственного интеллекта</p> <p>ПК-5.3. 3-3. Знает принципы работы распределенных кластерных систем</p> <p>ПК-5.3. У-1. Умеет решать задачи по выполнению коллективной проектной деятельности для создания, поддержки и использования системы искусственного интеллекта с применением машинного обучения и массово параллельных вычислений для ускорения машинного обучения</p> <p>ПК-5.3. У-2. Умеет работать с распределенной кластерной системой при создании, поддержке и использовании</p>
--	--	---

## 1.1. Текущий контроль успеваемости

Текущий контроль успеваемости осуществляется путем оценки результатов выполнения заданий практических (семинарских) занятий, самостоятельной работы, предусмотренных учебным планом и посещения занятий/активность на занятиях.

В качестве оценочных средств текущего контроля успеваемости предусмотрены:

Основным средством текущего контроля являются задания в формате решения теоретических задач и выполнения моделирования с помощью соответствующего программного обеспечения (Python, Exonum).

Пример задания:

- Найти сериализуемые истории в наборе транзакций, сгенерировать секретный ключ для Алисы и Боба в протоколе Диффи-Хеллмана, найти секрет схемы Блекли.
- Разработать и исследовать реализацию функции Proof-of-Work, которая принимает заголовок текущего блока и сложность вычисления блока в качестве входных данных и возвращает одноразовый номер для этого блока и заголовок добытого блока

Ученики получают баллы по результатам Домашних заданий. Максимальное количество баллов -100. Каждое задание Дает равный вклад в итоговую оценку. Очки за каждое задание зависят от его полноты. Проблема не встречалась - 0 баллов. Задание полностью выполнено - максимальное количество баллов соответствует ему.

Финальная презентация по групповому проекту и отчеты.

Пример: Задача состоит в том, чтобы внедрить игрушечную криптовалюту без наличных денег. То есть реализовать ключи, транзакции и логику хранения Merkle и подготовить ее демонстрацию.

Максимальное количество баллов - 100. Если проект не завершен полностью или у него есть слабые места, учащиеся получают баллы в зависимости от полноты и общего качества проекта. Если проект не запущен, студент получает 0 баллов.

## **1.2. Промежуточная аттестация**

Промежуточная аттестация осуществляется в форме экзамена

В качестве средств, используемых на промежуточной аттестации предусматривается:

Билеты

## **1.3. Типовые задания для проведения промежуточной аттестации**

Вопросы к экзамену

1. Обзор технологии блокчейн, типы блокчейнов и промышленные примеры
2. Хеш-функции.
3. Электронная подпись (RSA, ECDSA, EdDSA)
4. Простейшая (абстрактная) модель блокчейна.
5. PoW, PoS, DPoS
6. Bitcoin.
7. Script – язык программирования
8. Разбор изменений в алгоритм консенсуса (soft fork)
9. Segregated witness
10. Ethereum
11. Smart контракты
12. Разбор векторов атак на блокчейн, а также реализованные атаки.
13. Консенсус и невозможность распределенного консенсуса с одним ошибочным процессом (теорема).
14. Сетевые и вычислительные предположения (теорема).
15. Консенсусные свойства и примеры.
16. Атомная трансляция.
17. Tendermint. Eronum.
18. Криптовалюта, Сертификация, Анкеровка. Промышленные примеры

## 2. КРИТЕРИИ ОЦЕНКИ ПО ДИСЦИПЛИНЕ

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине				
Оценка	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
виды оценочных средств				
<b>Знания</b> (виды оценочных средств: приведены в п. 1.2.)	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
<b>Умения</b> (виды оценочных средств: приведены в п. 1.2.)	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности не принципиального характера)	Успешное и систематическое умение
<b>Навыки</b> (владения, опыт деятельности) (виды оценочных средств: приведены в п. 1.2..)	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач