

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**  
федеральное государственное автономное образовательное учреждение  
высшего образования  
«Балтийский федеральный университет имени Иммануила Канта»  
Высшая школа компьютерных наук и искусственного интеллекта

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Технология блокчейн**

**Шифр: 02.03.02**

**Направление подготовки: Фундаментальная информатика и информационные  
технологии**

**Профиль: Программная инженерия в искусственном интеллекте**

**Квалификация (степень) выпускника: бакалавр**

Калининград  
2023

## Лист согласования

**Составитель:** Верещагин Михаил Дмитриевич, к.ф.-м.н, директор Высшей школы компьютерных наук и искусственного интеллекта

Рабочая программа утверждена на заседании Учебно-методического совета (УМС)

Протокол № 33 от «27» октября 2023 г.

Профессор, д.ф.-м.н.,  
руководитель ОНК «Институт высоких технологий»

А.В. Юров

Директор высшей школы компьютерных наук  
и искусственного интеллекта

М.Д. Верещагин

Руководитель ОПОП ВО

С.С. Головин

## Содержание

1. Наименование дисциплины «Технология блокчейн».
2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.
3. Место дисциплины в структуре образовательной программы.
4. Виды учебной работы по дисциплине.
5. Содержание дисциплины, в том числе практической подготовки в рамках дисциплины, структурированное по темам.
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.
7. Методические рекомендации по видам занятий
8. Фонд оценочных средств
  - 8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины
  - 8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности в процессе текущего контроля
  - 8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине
  - 8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания
9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

## 1. Наименование дисциплины: Технология блокчейн.

**Цель дисциплины:** дать обзор понятия блокчейна и криптографии.

## 2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПК-5. Способен использовать инструментальные средства для решения задач машинного обучения	ПК-5.1. Осуществляет оценку и выбор инструментальных средств для решения поставленной задачи ПК-5.2. Разрабатывает модели машинного обучения для решения задач ПК-5.3. Создает, поддерживает и использует системы искусственного интеллекта, включающие разработанные модели и методы, с применением выбранных инструментов машинного обучения	<b>Знать:</b> возможности современных инструментальных средств и систем программирования для решения задач анализа данных и машинного обучения <b>Уметь:</b> проводить сравнительный анализ и осуществлять выбор инструментальных средств для решения задач машинного обучения <b>Владеть:</b> функциональными возможностями современных инструментальных средств и систем программирования в области создания моделей и методов машинного обучения ПК-интеллекта с применением машинного обучения и массово параллельных вычислений для ускорения машинного обучения

## 3. Место дисциплины в структуре образовательной программы

«Технология блокчейн» представляет собой дисциплину обязательной части (Б1.В.ДВ.05) направления подготовки бакалавриата 02.03.02 «Фундаментальная информатика и информационные технологии», профиль «Программная инженерия в искусственном интеллекте».

## 4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством

электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

## 5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование разделов (тем) дисциплины	Содержание разделов (тем) дисциплин
•	Введение в технологию блокчейн	Обзор технологии блокчейн, типы блокчейнов и промышленные примеры
•	Абстрактная модель блокчейна.	Хеш-функции. Электронная подпись (RSA, ECDSA, EdDSA) Простейшая (абстрактная) модель блокчейна. PoW, PoS, DPoS
•	Bitcoin и Ethereum.	Bitcoin. Script – язык программирования Разбор изменений в алгоритм консенсуса (soft fork) Segregated witness Ethereum Smart контракты Разбор векторов атак на блокчейн, а также реализованные атаки.
•	Практический обзор технологий блокчейна	Консенсус и невозможность распределенного консенсуса с одним ошибочным процессом (теорема). Сетевые и вычислительные предположения (теорема). Консенсусные свойства и примеры. Атомная трансляция. Tendermint. Eхonum. Криптовалюта, Сертификация, Анкеровка. Промышленные примеры

## 6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№ п/п	Наименование разделов (тем) дисциплины	Тема лекции
•	Введение в технологию блокчейн	Лекция 1 «Введение в технологию блокчейн».
•	Абстрактная модель блокчена.	Лекция 2 «Абстрактная модель блокчена»
•	Bitcoin и Ethereum.	Лекция 3 «Bitcoin и Ethereum»
•	Практический обзор технологий блокчейна	Лекция 4 «Практический обзор технологий блокчейна»

### Рекомендуемая тематика практических занятий:

1. Введение в технологию блокчейн
2. Абстрактная модель блокчена.
3. Bitcoin и Ethereum
4. Практический обзор технологий блокчейна

### Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на лабораторных занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации

преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

## **7. Методические рекомендации по видам занятий**

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Лабораторные занятия.

На лабораторных занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

## **8. Фонд оценочных средств**

### **8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины**

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно

связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Введение в технологию блокчейн	ПК-5	Опрос
Абстрактная модель блокчейна.	ПК-5	Опрос
Bitcoin и Ethereum.	ПК-5	Опрос
Практический обзор технологий блокчейна	ПК-5	Опрос

## 8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

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

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.

## 8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

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

#### 8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шкала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	<i>Включает нижестоящий уровень.</i> Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по	<i>Включает нижестоящий уровень.</i> Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и	хорошо		71-85

	образцу с большей степени самостоятель ности и инициативы	иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетвори тельный (достаточно й)	Репродуктивн ая деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетвор ительно		55-70
Недостаточн ый	Отсутствие удовлетворительного уровня	признаков	неудовлетв орительно	не зачтено	Менее 55

## 9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

### Основная литература

1. Криптографические основы блокчейн-технологий : практическое руководство / Е. А. Ищукова, С. П. Панасенко, К. С. Романенко, В. Д. Салманов. - Москва : ДМК Пресс, 2022. - 302 с. - ISBN 978-5-97060-865-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2109577> (дата обращения: 17.11.2023). – Режим доступа: по подписке.
2. Цихилов, А. М. Блокчейн : Принципы и основы : практическое руководство / А. М. Цихилов. - Москва : Интеллектуальная Литература, 2019. - 188 с. - ISBN 978-5-6042880-1-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1874893> (дата обращения: 17.11.2023). – Режим доступа: по подписке.
3. Генкин, А. Блокчейн: Как это работает и что ждет нас завтра : монография / А. Генкин, А. Михеев. - Москва : Альпина Паблишер, 2018. - 592 с. - ISBN 978-5-9614-6558-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1874894> (дата обращения: 18.11.2023). – Режим доступа: по подписке.

### Дополнительная литература

1. M.Swan Blockchain: Blueprint for a New Economy. O'REILLY 2015
2. B. Schneier Practical cryptography Wiley 2003

## 10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы

- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- ЭБС IBOOKS.RU
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантиана (<https://elib.kantiana.ru/>)

## **11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.**

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – [www.lms.kantiana.ru](http://www.lms.kantiana.ru), обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 10, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- GNU C++;
- Oracle Java;
- Deductor.
- среда разработки (JVE), компилятор (JVK) и виртуальная машина для исполнения кода (JVM) фирмы Oracle.
- Python 2.7.15 (Anaconda2 5.2.0 64-bit)
- Python 3.6.5 (Anaconda3 5.2.0 64-bit)
- 

## **12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.**

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.