

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

 Е.А. Турилова

28 февраля 2025 г.

подписано электронно-цифровой подписью

Программа дисциплины

Технологии распределенных реестров

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО
2. Место дисциплины (модуля) в структуре ОПОП ВО
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
 - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)
 - 4.2. Содержание дисциплины (модуля)
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
7. Перечень литературы, необходимой для освоения дисциплины (модуля)
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины (модуля) к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
13. Приложение №1. Фонд оценочных средств
14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)
15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и): старший преподаватель, б/с Хайруллин А.Ф. (кафедра теоретической кибернетики, отделение фундаментальной информатики и информационных технологий), Alfred.Khairoullin@kpfu.ru

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-1	Способность применять математические методы и модели в области информационной безопасности.

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

основные понятия и принципы технологии распределенных реестров

Должен уметь:

писать простые и сложные смарт-контракты на одном из существующих языков блокчейн систем

Должен владеть:

инструментами использования кошельков и разработки смарт-контрактов блокчейн систем

Должен демонстрировать способность и готовность:

использовать технологии распределенных реестров при разработке приложений

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.05.01 Дисциплины (модули)" основной профессиональной образовательной программы 10.04.01 "Информационная безопасность (Математические методы и программные технологии защиты информации)" и относится к дисциплинам по выбору части ОПОП ВО, формируемой участниками образовательных отношений.

Осваивается на 2 курсе в 3 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) на 72 часа(ов).

Контактная работа - 48 часа(ов), в том числе лекции - 0 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 48 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 24 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 3 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Се- местр	Виды и часы контактной работы, их трудоемкость (в часах)						Само- стоя- тель- ная ра- бота
			Лекции, всего	Лекции в эл. форме	Практи- ческие занятия, всего	Практи- ческие в эл. форме	Лабора- торные работы, всего	Лабора- торные в эл. форме	
1.	Тема 1. Основы технологии распределенных реестров	3	0	0	0	0	20	0	8
2.	Тема 2. Инструменты и языки разработки смарт-контрактов	3	0	0	0	0	14	0	8

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)						Самостоятельная работа
			Лекции, всего	Лекции в эл. форме	Практические занятия, всего	Практические в эл. форме	Лабораторные работы, всего	Лабораторные в эл. форме	
3.	Тема 3. Токены. ICO. DAO. Разработка распределенных приложений	3	0	0	0	0	14	0	8
	Итого		0	0	0	0	48	0	24

4.2 Содержание дисциплины (модуля)

Тема 1. Основы технологии распределенных реестров

Использование криптографии в технологии распределенных реестров. Простое шифрование. Ассиметричное шифрование. Хэширование. Приватный и публичный ключи. Цифровая подпись.

Основы технологий распределенных реестров. Криптовалюты. Алгоритмы консенсуса. Мифы о криптовалютах. Атаки на криптовалюты. Обзор криптовалют.

Тема 2. Инструменты и языки разработки смарт-контрактов

Инструменты разработки смарт-контрактов. Документация, среды разработки. Публичные и приватные сети. Базовые типы Solidity. Ключевые слова. Обработка ошибок.

Структура смарт-контракта. Описание переменных. Массивы, ассоциативные массивы (mapping). Адреса. Конструкторы. Переменная msg, её свойства. Контракты. Наследование и модификаторы.

Тема 3. Токены. ICO. DAO. Разработка распределенных приложений

Виды токенов. Базовый токен. Пример смарт-контракта базового токена.

Стандарт ERC-20. Смарт-контракт токена по стандарту ERC20.

Что такое ICO. Этапы ICO. Структура смарт-контракта для ICO. Реализация основных функций смарт-контракта для ICO.

Что такое DAO. Структура смарт-контракта для DAO. Один из примеров смарт-контракта для DAO.

Распределенные приложения Dapp.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства науки и высшего образования Российской Федерации от 6 апреля 2021 года №245)

Письмо Министерства образования Российской Федерации №14-55-99бин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;
- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Введение в криптовалюты и блокчейн - <https://www.intuit.ru/studies/courses/3443/685/info>

Работа с Ethereum - <https://www.intuit.ru/studies/courses/3630/872/info>

Технологии криптовалют - <https://www.intuit.ru/studies/courses/3643/885/info>

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лабораторные работы	Целью практических занятий является углубление и закрепление теоретических знаний, полученных студентами на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков. В ходе подготовки к практическому занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить заданные преподавателем практические задания. Желательно при подготовке к практическим занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.
самостоятельная работа	В рамках самостоятельной работы студенты выбирают для себя тему из предложенных преподавателем, проводят самостоятельное изучение этой темы по разным источникам, готовят презентацию и выступают с ней на занятиях. Кроме того, каждый выбирает некоторую тему для создания смарт-контракта на языке Solidity, и разрабатывает его в тестовой среде Sepolia экосистемы Ethereum.

Вид работ	Методические рекомендации
зачет	По дисциплине предусмотрен зачет, который также предусматривает тщательную работу с конспектом, основной и дополнительной литературой. Рекомендуется по каждому вопросу программы составить небольшое эссе, чтобы четко и систематизировано представить задачу, акцентировать внимание на ее свойствах и основных методиках их решений. Также следует повторно решить большинство типовых задач, так как они могут быть использованы в качестве дополнительных вопросов в случае спорных оценок.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

Компьютерный класс.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи;
- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.04.01 "Информационная безопасность" и магистерской программе "Математические методы и программные технологии защиты информации".

*Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.05.01 Технологии распределенных реестров*

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Основная литература:

Дрешер Д., Основы блокчейна: вводный курс для начинающих в 25 небольших главах [Электронный ресурс] / Дрешер Д., пер. с англ. А. В. Снастина. - М. : ДМК Пресс, 2018. - 312 с. - ISBN 978-5-97060-591-2 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785970605912.html>

Введение в криптографию. Курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. - М. : ФОРУМ : ИНФРА-М, 2018. - 240 с. - Режим доступа: <http://znanium.com/catalog/product/924700>

Дополнительная литература:

Блокчейн: Как это работает и что ждет нас завтра: Научно-популярное / Генкин А., Михеев А. - М.: Альпина Паблишер, 2018. - 592 с.: ISBN 978-5-9614-6558-7 - Режим доступа: <http://znanium.com/catalog/product/1002003>

Сажина М.А. Блокчейн в системе управления знанием : монография / М.А. Сажина, С.В. Костин. - М. : ИД 'ФОРУМ' : ИНФРА-М, 2019. - 90 с. - (Научная мысль). - Режим доступа: <http://znanium.com/catalog/product/989037>

Заколдаев, Д.А. ТЕХНОЛОГИЯ БЛОКЧЕЙН В РОССИИ: ДОСТИЖЕНИЯ И ПРОБЛЕМЫ [Электронный ресурс] / Д.А. Заколдаев, Р.В. Ямщиков, Н.В. Ямщикова. // Вестник Московского государственного областного университета (электронный журнал). - Электрон. дан. - 2018. - № 2. - С. 93-107. - Режим доступа: <https://e.lanbook.com/journal/issue/309469>

Грошева, Е.К. БЛОКЧЕЙН - НОВАЯ РЕВОЛЮЦИЯ [Электронный ресурс] / Е.К. Грошева, П.И. Невмержицкий. // Бизнес-образование в экономике знаний. - Электрон. дан. - 2018. - № 1. - С. 17-23. - Режим доступа: <https://e.lanbook.com/journal/issue/307707>

*Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.05.01 Технологии распределенных реестров*

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.