

**Федеральное государственное автономное образовательное  
учреждение высшего образования  
«Московский физико-технический институт  
(национальный исследовательский университет)»**

**УТВЕРЖДЕНО**  
**Директор**

**А.В. Малеев**

	<b>Рабочая программа дисциплины (модуля)</b>
<b>по дисциплине:</b>	Криптография. Часть 2
<b>по направлению:</b>	Программная инженерия
<b>профиль подготовки:</b>	Разработка программно-информационных систем высшая школа программной инженерии высшая школа программной инженерии
<b>курс:</b>	4
<b>квалификация:</b>	бакалавр

Семестр, формы промежуточной аттестации: 8 (весенний) - Экзамен

Аудиторных часов: 60 всего, в том числе:

лекции: 30 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 18 час.

Подготовка к экзамену: 30 час.

Всего часов: 108, всего зач. ед.: 3

Программу составил: А.А. Жмуров, канд. физ.-мат. наук, доцент

Программа обсуждена на заседании высшей школы программной инженерии 19.03.2025

## Аннотация

Курс знакомит слушателей с фундаментальными понятиями Блокчейн, современными проблемами различных разделов Блокчейн, основными свойствами и возможностями Блокчейн, а также методами и подходами для решения типовых прикладных задач.

### 1. Цели и задачи

#### Цель дисциплины

освоение основных понятий Блокчейн.

#### Задачи дисциплины

- Освоение студентами базовых знаний, понятий и концепций Блокчейн, блокчейн-платформ;
- Приобретение теоретических знаний и практических умений и навыков работы с различными блокчейн-платформами.

### 2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
ОПК-1 Способен применять естественнонаучные и общетехнические знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-6 Способен разрабатывать алгоритмы и программы, пригодные для практического использования, применять основы информатики и программирования к проектированию, конструированию и тестированию программных продуктов	ОПК-6.3 Знает методы тестирования программного кода на ошибки и способен проводить тестирование на различных уровнях (модульное, интеграционное, системное)
ОПК-7 Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой	ОПК-7.1 Обладает навыками создания и выполнения тестовых сценариев для выявления ошибок в программном обеспечении
	ОПК-7.2 Понимает принципы работы баз данных и умеет проектировать структуру данных для эффективного хранения информации
ОПК-8 Способен осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	ОПК-8.1 Понимает принципы, по которым работают базы данных, и умеет создавать структуру данных, оптимизированную для эффективного хранения и обработки информации
	ОПК-8.3 Умеет оптимизировать и проводить рефакторинг существующего кода для улучшения производительности и поддержки
	ОПК-8.2 Умеет применять технологии машинного обучения в различных прикладных областях
ПК-3 Способен проектировать, разрабатывать, интегрировать, проверять на работоспособность программное обеспечение	ПК-3.2 Умеет выбирать языки программирования для написания программного кода с учетом технического задания

### 3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

фундаментальные понятия Блокчейн;  
современные проблемы соответствующих разделов Блокчейн;  
основные свойства и возможности Блокчейн;  
методы и подходы для решения типовых прикладных задач.

уметь:

понять поставленную задачу;  
использовать свои знания для решения фундаментальных и прикладных задач;  
оценивать корректность постановок задач;  
самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;  
самостоятельно видеть следствия полученных результатов.

владеть:

навыками освоения большого объема информации и решения задач (в том числе, сложных);  
навыками самостоятельной работы и освоения новых дисциплин;  
культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования изученных подходов и методов;  
предметным языком и навыками грамотного описания решения задач и представления полученных результатов.

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

##### 4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Криптография с открытым ключом. Основные механизмы, задачи и проблемы	3	3		2
2	Математические основы криптографии с открытым ключом	3	3		2
3	Базовые сложные математические задачи криптографии с открытым ключом	3	3		2
4	Шифрование с открытым ключом	3	3		2
5	Электронная подпись	3	3		2
6	Инфраструктура открытых ключей	3	3		2
7	Протоколы аутентифицированной выработки общего ключа	4	4		2
8	Защищенное использование закрытого ключа и PAKE-протоколы	4	4		2
9	Протокол TLS	4	4		2
Итого часов		30	30		18
Подготовка к экзамену		30 час.			
Общая трудоёмкость		108 час., 3 зач.ед.			

##### 4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 8 (Весенний)

## 1. Криптография с открытым ключом. Основные механизмы, задачи и проблемы

Введение в криптографию с открытым ключом: основные принципы, отличие от симметричных методов, ключевые задачи (шифрование, цифровая подпись, аутентификация), проблемы безопасности и устойчивости.

## 2. Математические основы криптографии с открытым ключом

Разбор фундаментальных математических концепций, используемых в асимметричной криптографии: теории чисел, модульной арифметики, алгебры конечных полей и эллиптических кривых.

## 3. Базовые сложные математические задачи криптографии с открытым ключом

Анализ криптографических задач, лежащих в основе алгоритмов с открытым ключом: факторизация целых чисел, дискретное логарифмирование, задача решетки и их влияние на безопасность алгоритмов.

## 4. Шифрование с открытым ключом

Рассмотрение основных схем шифрования с открытым ключом (RSA, ElGamal, ECC), их архитектуры, преимуществ, уязвимостей и областей применения.

## 5. Электронная подпись

Принципы работы цифровой подписи, её назначение, алгоритмы (DSA, ECDSA, RSA-PSS), а также механизмы защиты от подделки и подмены данных.

## 6. Инфраструктура открытых ключей

Описание PKI (Public Key Infrastructure), управления сертификатами, центров сертификации (CA), моделей доверия и механизмов отзыва сертификатов.

## 7. Протоколы аутентифицированной выработки общего ключа

Изучение методов безопасного согласования ключей между сторонами (Diffie-Hellman, ECDH), их аутентифицированных версий и применения в защищенных соединениях.

## 8. Защищенное использование закрытого ключа и PAKE-протоколы

Методы защиты закрытых ключей, аппаратные и программные механизмы хранения, а также протоколы аутентификации с подтверждением пароля (PAKE: SRP, EKE, SPAKE2).

## 9. Протокол TLS

Структура и механизмы работы TLS (Transport Layer Security): установление защищенного соединения, этапы рукопожатия, алгоритмы шифрования и аутентификации, версия TLS 1.3 и её отличия.

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

Стандартная учебная аудитория, оборудованная проектором, экраном и маркерной доской.

## **6.Перечень рекомендуемой литературы**

#### Основная литература

Фонд библиотеки МФТИ:

1. Рацеев, С. М. Криптография. Безопасные многосторонние вычисления : учебное пособие для вузов / С. М. Рацеев. — Санкт-Петербург : Лань, 2025. — 468 с. — ISBN 978-5-507-50213-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/440033>
2. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/206285>

#### Дополнительная литература

-

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

<https://cryptomoney.ru/>  
<https://habr.com/>

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

Не предусмотрено.

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

1. Для овладения дисциплиной рекомендуется посещать лекции, успешно сдавать контрольные и практические работы, решать практические задачи, так как это упрощает итоговую аттестацию по предмету.
2. Для подготовки к итоговой аттестации по предмету лучше всего пользоваться электронными материалами, предоставленными преподавателем.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

**по направлению:** Программная инженерия  
**профиль подготовки:** Разработка программно-информационных систем  
высшая школа программной инженерии  
высшая школа программной инженерии  
**курс:** 4  
**квалификация:** бакалавр

Семестр, формы промежуточной аттестации: 8 (весенний) - Экзамен

**Разработчик:** А.А. Жмуров, канд. физ.-мат. наук, доцент

## 1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
ОПК-1 Способен применять естественнонаучные и общетехнические знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-6 Способен разрабатывать алгоритмы и программы, пригодные для практического использования, применять основы информатики и программирования к проектированию, конструированию и тестированию программных продуктов	ОПК-6.3 Знает методы тестирования программного кода на ошибки и способен проводить тестирование на различных уровнях (модульное, интеграционное, системное)
ОПК-7 Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой	ОПК-7.1 Обладает навыками создания и выполнения тестовых сценариев для выявления ошибок в программном обеспечении
	ОПК-7.2 Понимает принципы работы баз данных и умеет проектировать структуру данных для эффективного хранения информации
ОПК-8 Способен осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	ОПК-8.1 Понимает принципы, по которым работают базы данных, и умеет создавать структуру данных, оптимизированную для эффективного хранения и обработки информации
	ОПК-8.3 Умеет оптимизировать и проводить рефакторинг существующего кода для улучшения производительности и поддержки
	ОПК-8.2 Умеет применять технологии машинного обучения в различных прикладных областях
ПК-3 Способен проектировать, разрабатывать, интегрировать, проверять на работоспособность программное обеспечение	ПК-3.2 Умеет выбирать языки программирования для написания программного кода с учетом технического задания

## 2. Показатели оценивания компетенций

В результате изучения дисциплины «Криптография. Часть 2» обучающийся должен:

### знать:

фундаментальные понятия Блокчейн;  
современные проблемы соответствующих разделов Блокчейн;  
основные свойства и возможности Блокчейн;  
методы и подходы для решения типовых прикладных задач.

### уметь:

понять поставленную задачу;  
использовать свои знания для решения фундаментальных и прикладных задач;  
оценивать корректность постановок задач;  
самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;  
самостоятельно видеть следствия полученных результатов.

### владеть:

навыками освоения большого объема информации и решения задач (в том числе, сложных);  
навыками самостоятельной работы и освоения новых дисциплин;  
культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования изученных подходов и методов;  
предметным языком и навыками грамотного описания решения задач и представления полученных результатов.

### **3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю**

Не предусмотрено.

### **4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся**

9 семестр

1) Пояснить смысл основных понятий Блокчейн:

- Цепочка блоков
- Private и public keys
- Консенсус
- Публичные и приватные блокчейны
- Ациклические направленные графы
- Форки
- Смартконтракты
- Транзакции
- UTXO модель
- Структура блока
- Merkle tree
- Timestamp
- Nonce – расчет хеша
- Управление сложностью
- Майнинг
- Omni Layer
- Lightning Network
- Платежные каналы
- Неподтвержденные транзакции
- Защита от двойной платы
- Мультиподпись
- Хеши и секреты
- Двунправленные платежные каналы
- Контракты с хешированием и временной блокировкой
- Фиксация состояния
- Заккрытие канала

2) Схема работы блокчейна.

3) CAP – теорема (теорема Брюера).

4) P2p облака транзакций.

5) Валидаторы.

6) Скорость обработки транзакций.

7) Лэтенси.

8) Альтернативные схемы.

9) Atomic Swap, Decred и Litecoin, BTC и ETH.

10) Платформа Qtum.

11) Атомарные свопы.

12) Public и private blockchains, permission и permissionless.

13) Аккаунтная модель.



10 семестр

14) Виды атак на блокчейны.

15) DAG.

16) Проекты IOTA, Byteball, Hedera Hashgraph, Universa (гибридный вариант).

17) Tendermint, Форк vs Конструктор

18) Создание блокчейн на Tendermint.

19) EOS, Stellar, Custody сервисы, Мультиподписи, Sharding.

20) Доказательство с нулевым разглашением.

Примеры экзаменационных билетов в 10 семестре:

Билет 1.

1. Виды атак на блокчейны.

2. Создание блокчейн на Tendermint.

Билет 2.

1. DAG.

2. Доказательство с нулевым разглашением.

#### Критерии оценивания

- оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений
- оценка «хорошо (7)» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (6)» выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (5)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач
- оценка «неудовлетворительно (1)» выставляется студенту, который не знает формулировок основных понятий дисциплины

#### 5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения дифференцированного зачета и устного экзамена обучающиеся могут пользоваться программой дисциплины.