МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное

учреждение высшего образования «Южный федеральный университет»

(ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ)

УТВЕРЖДАЮ

Директор Института компьютерных технологий и информационной безопасности

\_\_\_\_\_\_\_\_\_\_\_\_ /Г.Е. Веселов /

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Криптографические протоколы для современных блокчейн систем**

Ростов-на-Дону – Таганрог 2021

**Составитель рабочей программы:**

К.т.н., доцент каф. БИТ ИКТИБ ЮФУ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Е. А. Ищукова /

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г.

Программа одобрена на заседании УМС Института компьютерных технологий и информационной безопасности

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г., протокол № \_\_\_\_\_

**Председатель УМС ИКТИБ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / А. Е. Лызь /

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г.

Содержание

[I. Цели и задачи освоения дисциплины 4](#_Toc64275489)

[II. Место дисциплины в структуре образовательной программы 4](#_Toc64275490)

[III. Требования к результатам освоения дисциплины 5](#_Toc64275491)

[IV. Содержание и структура дисциплины 6](#_Toc64275492)

[4.1. План внеаудиторной самостоятельной работы 9](#_Toc64275494)

[4.2. Содержание учебного материала 13](#_Toc64275495)

[V. Образовательные технологии 15](#_Toc64275496)

[VI. Учебно-методическое обеспечение дисциплины 15](#_Toc64275497)

[6.1. Основная литература 15](#_Toc64275498)

[6.2. Дополнительная литература 15](#_Toc64275499)

[6.3. Перечень ресурсов сети Интернет 16](#_Toc64275500)

[VII. Материально-техническое обеспечение дисциплины 16](#_Toc64275501)

[VIII. Методические указания для обучающихся по освоению дисциплины 16](#_Toc64275502)

[IX. Учебная карта дисциплины 18](#_Toc64275503)

[X. Фонд оценочных средств 19](#_Toc64275504)

[10.1. Паспорт фонда оценочных средств 19](#_Toc64275505)

[10.2Доклады по модулям1 и 2 19](#_Toc64275506)

[10.3 Практические задания 25](#_Toc64275507)

[10.4 Контрольные работы по модулям 1 и 2 34](#_Toc64275508)

# Цели и задачи освоения дисциплины

Цели освоения дисциплины:

* формирование у студентов базовых знаний в области проектирования, разработки и особенностей применения современных криптографических протоколов при проектировании блокчейн систем различного назначения.

Задачи освоения дисциплины:

* сформировать представление об основных задачах и понятиях современных криптографических протоколов, применяемых в блокчейн системах;
* изучить протоколы, используемые для обеспечения работы блокчейн систем;
* изучить также форматы, используемые для механизмов консенсуса, механизмов коллективной подписи, механизмов подписи и распространения транзакций, в том числе вслепую, а также решения иных задач, в том числе для защиты блокчейн систем;
* освоить основные приемы построения и использования протоколов, предназначенных для блокчейн систем;
* получить представление о способе анализа защищенности применяемых криптографических протоколов;
* раскрыть свойства безопасности протоколов;
* дать представление об уязвимостях блокчейн систем;

# Место дисциплины в структуре образовательной программы

Дисциплина относится к модулю профессиональных дисциплин, формируемого участниками образовательных отношений, образовательной программы.

Данная дисциплина опирается на базовые знания, умения и навыки, формируемые при получении предшествующего уровня образования.

Знания, умения и навыки, формируемые данной дисциплиной, потребуются в научно-исследовательской работе магистрантов, при выполнении выпускных квалификационных работ, а также в дальнейшей профессиональной деятельности.

# Требования к результатам освоения дисциплины

Освоение дисциплины направлено на формирование следующих компетенций в соответствии с образовательным стандартом и образовательной программой:

Перечень планируемых результатов обучения по дисциплине, соотнесённых с индикаторами достижения компетенций

| Компетенция | Индикаторы достижения компетенции | Результаты обучения |
| --- | --- | --- |
| ВПК-1. Способен создавать и исследовать решения различного назначения на базе технологии блокчейн | ВПК-1.1. Выбирает необходимый криптографический протокол и выполняет его программную реализацию | Выполнение индивидуального задания по разработке и реализации блокчейн-системы с использованием заданных криптографических протоколов |
| ВПК-1.2. Выбирает механизм консенсуса, разрабатывает и реализует архитектуру безопасного блокчейн решения | Выполнение индивидуального задания по разработке и реализации блокчейн-системы с использованием заданных криптографических протоколов |

# Содержание и структура дисциплины

Трудоёмкость дисциплины составляет 8 зачётных единиц, 288часов,

в том числе 3 зачётных единицы, 108 часов с использованием онлайн-курса «Основы и практическое применение блокчейна» ([https://www.coursera.org/learn/blokcheyna](https://vk.com/away.php?to=https%3A%2F%2Fwww.coursera.org%2Flearn%2Fblokcheyna&cc_key=))

Форма промежуточной аттестации: практикоориентированный экзамен

Содержание дисциплины, структурированное по темам

| № п/п | Темы дисциплины | Семестр | Виды учебной работы и их трудоёмкость, часы  (в том числе с использованием онлайн-курсов) | | | | Наименования оценочных средств |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Контактная работа | | | Самостоя­тельная работа |
| Лекции | Практические занятия | Лабораторные занятия |
| **Модуль 1.** «Базовые протоколы для блокчейн систем» | | | | | | | |
| 1 | Тема 1. Криптографические методы для блокчейн-систем. Асимметричная криптография. Выработка ключей для асимметричных систем. ЭЦП, контроль целостности, дерево Меркля. | 3 | 6 | 4 | - | 26 | * работа на лекционных занятиях по модулю 1 (дискуссия); * практические занятия по модулю 1(защита практического задания№1 «Алгоритм RSA»). * Прохождение онлайн-курса «Основы и практическое применение блокчейна» |
| 2 | Тема 2. Протоколы консенсуса. Доказательство работы, доказательство доли, задача о византийских генералах и другие. | 3 | 4 | 4 | - | 22 | практические занятия по модулю 1 (защита практического задания№2 «. Поиск nonce для протокола консенсуса Доказательство работы.», «Прохождение онлайн-курса «Основы и практическое применение блокчейна» |
| 3 | Тема 3. Протоколы идентификации-аутентификации. Парольные схемы. Схемы типа «запрос-ответ». Протокол рукопожатия. | 3 | 4 | 4 | - | 22 | практические занятия по модулю 1 (защита практического задания№3 «Построение схемы аутентификации для заданной блокчейн-системы»).  Прохождение онлайн-курса «Основы и практическое применение блокчейна» |
| 4 | Тема 4. Протоколы распределенного хранения ключей. Китайская теорема об остатках. Схема Блекли. Схема Шамира. | 3 | 4 | 4 | - | 22 | практические занятия по модулю 1 (защита практического задания №4 «Распределение ключа по заданному протоколу»).  Прохождение онлайн-курса «Основы и практическое применение блокчейна» |
| **Модуль 2.**«Прикладные протоколы для блокчейн систем» | | | | | | | |
| 5 | Тема 5. Протоколы с нулевым разглашением знания. | 3 | 6 | 4 | - | 26 | практические занятия по модулю 2 (защита практического задания №5 «Основы реализации протокола с нулевым разглашением знания»).   * Прохождение онлайн-курса «Основы и практическое применение блокчейна» |
| 6 | Тема 6. Протоколы электронного голосования. Протоколы тайного электронного голосования. | 3 | 4 | 4 | - | 22 | практические занятия по модулю 2 (защита практического задания №6 «Основы реализации протокола электронного голосования»).   * Прохождение онлайн-курса «Основы и практическое применение блокчейна» |
| 7 | Тема 7. Протоколы распределения и обмена ключами | 3 | 4 | 4 | - | 22 | практические занятия по модулю 2 (защита практического задания №7 «Основы реализации протокола распределения ключа»).   * Прохождение онлайн-курса «Основы и практическое применение блокчейна» |
| 8 | Тема 8. Оракулы в области блокчейн-технологий | 3 | 4 | 4 | - | 22 | * практические занятия по модулю 2 (защита практического задания №8 «Построение схемы работы оракула для блокчейн-системы.») * Прохождение онлайн-курса «Основы и практическое применение блокчейна» |
| 9 | Практикоориентированный экзамен | 3 | - | 4 | - | 32 | Задание для экзамена, критерии оценки выполненного задания |
| **Итого часов** | | 3 | 36 | 36 | 0 | 212 | – |

## План внеаудиторной самостоятельной работы

| № п/п | Темы дисциплины | Семестр | Вид самостоятельной работы | Сроки выполнения (нед.) | Затраты времени (часы) | Учебно-методическое обеспечение |
| --- | --- | --- | --- | --- | --- | --- |
| **Модуль 1.** «Базовые протоколы для блокчейн систем» | | | | | | |
| 1 | Тема 1. Криптографические методы для блокчейн-систем. Асимметричная криптография. Выработка ключей для асимметричных систем. ЭЦП, контроль целостности, дерево Меркля. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания№1; * изучение материалов онлайн-курса «Основы и практическое применение блокчейна». | 1–3 | 26 | Задание к практической работе №1, основная и дополнительная литература, материалы онлайн курса «Основы и практическое применение блокчейна» |
| 2 | Тема 2. Протоколы консенсуса. Доказательство работы, доказательство доли, задача о византийских генералах и другие. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания№2; * изучение материалов онлайн-курса «Основы и практическое применение блокчейна». | 4–5 | 22 | Задание к практической работе №2, основная и дополнительная литература, материалы онлайн курса «Основы и практическое применение блокчейна» |
| 3 | Тема 3. Протоколы идентификации-аутентификации. Парольные схемы. Схемы типа «запрос-ответ». Протокол рукопожатия. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания№3; * изучение материалов онлайн-курса «Основы и практическое применение блокчейна». | 6-7 | 22 | Задание к практической работе №3, основная и дополнительная литература, материалы онлайн курса «Основы и практическое применение блокчейна» |
| 4 | Тема 4. Протоколы распределенного хранения ключей. Китайская теорема об остатках. Схема Блекли. Схема Шамира. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания№4; * изучение материалов онлайн-курса «Основы и практическое применение блокчейна». | 8-9 | 22 | Задание к практической работе №4, Основная и дополнительная литература, список тем докладов, материалы онлайн курса «Основы и практическое применение блокчейна» |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Модуль 2.** «Прикладные протоколы для блокчейн систем» | | | | | | |
| 5 | Тема 5. Протоколы с нулевым разглашением знания. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания№5; * изучение материалов онлайн-курса «Основы и практическое применение блокчейна». | 10-12 | 26 | Задание к практической работе №5, основная и дополнительная литература, материалы онлайн курса «Основы и практическое применение блокчейна» |
| 6 | Тема 6. Протоколы электронного голосования. Протоколы тайного электронного голосования. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания№6; * изучение материалов онлайн-курса «Основы и практическое применение блокчейна». | 13-14 | 22 | Задание к практической работе №6, основная и дополнительная литература, материалы онлайн курса «Основы и практическое применение блокчейна» |
| 7 | Тема 7. Протоколы распределения и обмена ключами | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №7; * изучение материалов онлайн-курса «Основы и практическое применение блокчейна». | 15-16 | 22 | Задание к практической работе №7, основная и дополнительная литература, список тем докладов, материалы онлайн курса «Основы и практическое применение блокчейна» |
| 8 | Тема 8. Оракулы в области блокчейн-технологий | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №8; * изучение материалов онлайн-курса «Основы и практическое применение блокчейна». | 17-18 | 22 | Задание к практической работе №8, основная и дополнительная литература, материалы онлайн курса «Основы и практическое применение блокчейна» |
| 9 | Практикоориентированный экзамен | 3 | * проработка и повторение материала лекционных занятий; * повторение материала практических заданий; * повторение материалов онлайн-курса «Основы и практическое применение блокчейна». | 19-21 | 32 | Задание к экзаену |
| **Общая трудоёмкость самостоятельной работы по дисциплине** | | | | | 212 | – |

## Содержание учебного материала

**Модуль 1. «Базовые протоколы для блокчейн систем»**

**4.3.1. Криптографические методы для блокчейн-систем. Асимметричная криптография. Выработка ключей для асимметричных систем. ЭЦП, контроль целостности, дерево Меркля.** Понятие криптографического протокола. Отличия криптографического протокола от криптографического алгоритма. Роль криптографических протоколов в блокчейн системах. Свойства протоколов, характеризующие их безопасность. Общая классификация криптографических протоколов: протоколы с посредником, протоколы с арбитром, самодостаточные протоколы. Основные виды уязвимостей. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные соглашения об участниках криптографических протоколов. Асимметричная криптография.Алгоритм шифрования RSA. Элиптическая криптография. Электронная цифровая подпись. Алгоритмы для контроля целостности документов. Функции хэширования. Дерево Меркля.

### **4.3.2. Протоколы консенсуса. Доказательство работы, доказательство доли, задача о византийских генералах и другие.** Доказательство работы (Proof-of-Work). Доказательство доли (Proof-of-Stake).  Делегированное доказательство доли (Delegated Proof-of-Stake (DPoS)). Делегированный протокол задачи византийских генералов (Delegated Byzantine Fault Tolerance (DBFT)).Реализация протокола задачи византийских генералов (Practical Byzantine Fault Tolerance (PBFT)). Федеративное византийское соглашение. (Federated Byzantine Agreement (FBA)). Направленный ациклический граф (Directed Acyclic Graph (DAG)).  ХэшГраф. (HashGraph).

**4.3.3. Протоколы идентификации-аутентификации. Парольные схемы. Схемы типа «запрос-ответ». Протокол рукопожатия.**

Понятие об идентификации. Классификация схем идентификации и аутентификации. Парольные схемы. Разновидности парольных схем. Требования к парольным схемам. Использование хэш-функций в парольных схемах. Одноразовые пароли. Схема Лампорта. Протоколы рукопожатия. Требования к протоколам рукопожатия. Область применения протоколов рукопожатия. Основные понятия и концепции. Аутентификация источника данных. Аутентификация сущности. Генерация аутентифицированных ключей. Механизм меток времени.

**4.3.4. Протоколы распределенного хранения ключей. Китайская теорема об остатках. Схема Блекли. Схема Шамира.**

Понятие схемы разделения секрета (СРС). Группа доступа. Структура доступа. Пороговые СРС – схема Шамира, схема Блекли, схема на основе Китайской теоремы об остатках. Разделение секрета для произвольной группы доступа. Совершенная СРС. Проверяемое разделение секрета. Протоколы конфиденциальных вычислений. Пример для схемы Шамира.

**Модуль 2. «Прикладные протоколы для блокчейн систем»**

**4.3.5. Протоколы с нулевым разглашением знания.**

Понятие об интерактивных системах доказательства (ИСД). Примеры ИСД (квадратичные невычеты; неизоморфизм графов). Примеры ИСД с нулевым разглашением (изоморфизм графов). Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Схема Шнорра. Схема Брикелла-МакКарли. Схема Окамото и теорема о ее условной стойкости. Схема Гиллу-Кискатр. Доказательства полноты и корректности этих схем.

**4.3.6. Протоколы электронного голосования. Протоколы тайного электронного голосования.**

Основные требования к системам голосования. Модель протокола с одной доверенной счетной комиссией. Протокол Шаума-Педерсона. Неинтерактивный протокол Шаума-Педерсона. Протокол голосования с несколькими счетными комиссиями. Проблемы систем голосования. Голосование через «слепые подписи». Система голосования с двумя избирательными комиссиями. Пример системы голосования с несколькими центрами. Проблемы арбитража. Слепая подпись. Затемненная подпись. Применение слепых подписей. Скрытый канал. Подписи со скрытым каналом. Скрытый канал на основе подписи Онга-Шнорра-Шамира. Подход к построению скрытого канала. Подписи, свободные от скрытого канала.

**4.3.7. Протоколы распределения и обмена ключами.**

Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами. Централизованная выработка ключа. Совместная выработка ключа. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра. Схемы Wide-MouthFrog, Yahalom, протокол Нидхема-Шредера, Отвея-Рииса. Бесключевой протокол Шамира. Протокол Диффи-Хэллмана. Протокол Нидхема-Шредера на основе шифра с открытым ключом. Протоколы передачи сеансовых секретных ключей. Протокол WideMouthFrog. Обмен зашифрованными ключами EKE. Трехпроходный протокол Шамира.

**4.3.8. Оракулы в области блокчейн-технологий.** Блокчейн-оракулы как связь между цифровым и реальным миром. Пример использования оракулов. Разновидности оракулов. Программные оракулы. Аппаратные оракулы. Входящие и исходящие оракулы. Централизованные и децентрализованные оракулы. [Контракто-ориентированные оракулы](https://academy.binance.com/ru/articles/blockchain-oracles-explained#contract-specific-oracles). Человек-оракул. Проблемные аспекты оракулов.

Перечень тем практических занятий

| №  п/п | Тема практического занятия | Количество часов |
| --- | --- | --- |
| **Модуль 1. «Базовые протоколы для блокчейн систем»** | | |
| 1 | Практическое задание №1 «Алгоритм RSA». | 6 |
| 2 | Практическое задание №2 «Поиск nonce для протокола консенсуса Доказательство работы». | 4 |
| 3 | Практическое задание №3 «Построение схемы аутентификации для заданной блокчейн-системы». | 4 |
| 4 | Практическое задание №4 «Распределение ключа по заданному протоколу». | 4 |
| **Модуль 2. «Прикладные протоколы для блокчейн систем»** | | |
| 5 | Практическое задание №5 «Основы реализации протокола с нулевым разглашением знания». | 6 |
| 6 | Практическое задание №6 «Основы реализации протокола электронного голосования». | 4 |
| 7 | Практическое задание №7 «Основы реализации протокола распределения ключа». | 4 |
| 8 | Практическое задание №8 «Построение схемы работы оракула для блокчейн-системы». | 4 |
| **Всего часов** | | **36** |

# Образовательные технологии

По дисциплине предусмотрены следующие методы обучения и интерактивные формы проведения занятий:

По дисциплине предусмотрены следующие активные формы обучения:

* лекции-визуализации – с использованием презентационного материала;
* практические занятия, в рамках которых обучающиеся делают доклады по заданным темам, обсуждаются вопросы выполнения практических заданий и представление проделанной работы.

Наряду с традиционными образовательными технологиями, для реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологий в электронной информационно-образовательной среде Южного федерального университета и образовательной платформы «Открытое образование» (https://openedu.ru). Лекционные занятия и другие формы контактной работы обучающихся с преподавателем могут проводиться с использованием платформы MicrosoftTeams, OneDriveи системы электронного обучения ИКТИБ ЮФУ (lms.sfedu.ru), что позволяет обеспечить онлайн и офлайн взаимодействие преподавателя с обучающимися в рамках дисциплины.

Основными методами контроля являются письменные контрольные работы, отчеты к практическим заданиям, презентации докладов, сертификат о прохождении онлайн курса «Защита информации», а также электронный учёт и контроль учебных достижений студентов (использование средств сервиса балльно-рейтинговой системы; ведение электронного журнала успеваемости и применение других средств контроля с использованием системы электронного обучения).

# Учебно-методическое обеспечение дисциплины

## Основная литература

1. Фролов А.В. Создание смарт-контрактов Solidity для блокчейна Ethereum. Практическое руководство / А. В. Фролов — «ЛитРес: Самиздат», 2019. – 258 с. / <https://www.litres.ru/aleksandr-frolov-198/sozdanie-smart-kontraktov-solidity-dlya-blokcheyna-et/chitat-onlayn/>

## Дополнительная литература

1. Satoshi Nakomoto Bitcoin: A Peer-to-Peer Electronic Cash System <https://bitcoin.org/bitcoin.pdf>
2. БиткоинВики <https://en.bitcoin.it/wiki/Main_Page>
3. Блокчейн изнутри: как устроен биткоин <https://vas3k.ru/blog/blockchain/>
4. Как устроен Ethereum и смарт-контракты <https://vas3k.ru/blog/ethereum/>
5. BaumankaCoin – велосипед в 3000 строк или блокчейн на пальцах<https://habr.com/ru/post/340206/>
6. Даниэль Дрешер Основы блокчейна: вводный курс для начинающих в 25 небольших главах / пер. с англ. А. В. Снастина. – М.: ДМК Пресс, 2018. – 312 с.: ил.

## Перечень ресурсов сети Интернет

* Хабрахабр. URL: http://habrahabr.ru/ (дата обращения: 29.05.2017).
* Informit. URL: http://www.informit.com (дата обращения: 29.05.2017).
* ru.wikipedia.org – Русская Википедия, для уточнения отдельных определений и алгоритмов(дата обращения: 29.05.2017).
* Сайт ЮФУ, <http://sfedu.ru/>
* Сайт Института компьютерных технологий и информационной безопасности, <http://ictis.sfedu.ru/>
* Научно-техническое отделение зональной научной библиотеки ЮФУ, г. Таганрог, <http://ntb.tti.sfedu.ru/>
* Электронная библиотечная система ЮФУ, <http://library.sfedu.ru>
* Сайт кафедры Безопасности информационных технологий, http://bit.ictis.sfedu.ru/

# Материально-техническое обеспечение дисциплины

При реализации дисциплины используются следующие помещения, оборудование и программное обеспечение:

1. аудитория лекционного типа:

* Компьютер преподавателя - 1 шт.;
* Экран для проектора с электроприводом – 1 шт.;
* Мультимедийный проектор – 1 шт.;
* Сетевое оборудование – 1 шт.;
* Microsoft Windows, Microsoft Office PowerPoint.

1. аудитория практических занятий, индивидуальных и групповых консультаций, промежуточной аттестации:

* Доска интерактивная – 1 шт.,
* Компьютер преподавателя – 1 шт.;
* Компьютер – 17 шт.;
* Сетевое оборудование – 1 шт.;
* OneDrive;
* Microsoft Teams;
* Система электронного обучения ИКТИБ ЮФУ(lms.sfedu.ru);
* Ubuntu, OpenOffice.

# Методические указания для обучающихся по освоению дисциплины

Учебный процесс обучения дисциплине включает в себя аудиторные занятия (лекции, практические занятия) и самостоятельную работу. Промежуточная аттестация по дисциплине – дифференциальный зачет. Лектор и преподаватели, ведущие занятия, контролируют посещение всех видов аудиторных занятий.

Чтение лекций проводится с демонстрацией слайдов. Материалы лекционных занятий (презентации), практических занятий и заданий своевременно предоставляются в пользование студентов посредством размещения в электронном пространстве (облачные хранилища –OneDrive, lms.sfedu.ru, MicrosoftTeams).

Практические занятия проводятся в аудитории, оснащенной интерактивной доской, и иллюстрируются презентациями и наглядной демонстрацией выполнения соответствующих задач. Практические занятия требуют предварительной теоретической подготовки по соответствующей теме: изучения основной и дополнительной литературы по дисциплине. На практических занятиях осуществляется периодические дискуссии по ранее изученному материалу, обучающиеся делают доклады по темам практических занятий, преподаватель разбирает качество сделанных докладов, осуществляется разбор практических заданий и обзор выполнения контрольной работы.

Самостоятельная работа студентов включает в себя подготовку к лекционным, практическим занятиям, контрольным работам, выполнение практических заданий, а так еж изучение материалов онлайн-курса «Основы и практическое применение блокчейна». Контроль усвоения материала осуществляется на аудиторных занятиях путем обсуждения теоретического материала по теме занятия, обсуждения вопросов, разобранных по предыдущей теме, при проверке и защите практических заданий и контрольный работ.

Максимальное количество баллов по каждому виду работ указано в учебной карте дисциплины.

Студенты, которые по уважительной причине не смогли набрать необходимое число баллов по текущему и рубежному контролю модуля, могут по согласованию с преподавателем ликвидировать задолженности до конца последней недели обучения соответствующего семестра.

# Учебная карта дисциплины

Курс 2, семестр3, очная форма обучения

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Виды контрольных мероприятий  (наименования оценочных средств) | Количество баллов | |
| Текущий контроль | Рубежный контроль |
| Модуль 1. Основы защиты информации в компьютерных системах | | | |
| 1 | Практическое занятие №1 |  | - |
| 3 | Практическое занятие №2 |  | - |
| 4 | Практическое занятие №3 |  | - |
| 5 | Практическое занятие №4 |  |  |
| 6 | Контрольная работа по модулю 1 | - | 10 |
| Модуль 2. Методология обеспечения и оценки безопасности информационных систем | | | |
| 7 | Практическое занятие №5 |  | - |
| 8 | Практическое занятие №6 |  | - |
| 9 | Практическое занятие №7 |  |  |
| 10 | Практическое занятие №8 |  |  |
| 11 | Контрольная работа по модулю 2. | - | 10 |
| **Всего** | | 40 | 20 |
| Бонусные баллы | | 10 баллов  Бонусные баллы назначаются за успешное прохождение онлайн-курса «Основы и практическое применение блокчейна» (набрано более 85 баллов) | |
| **Промежуточная аттестация  в форме экзамена** | | 40 баллов  Экзамен проводится в практикоориентированном виде. Студенты выполняют задание в течение 4 часов. Оценка за выполненное задание ставится в соответствии с критериями оценивания.  Минимальное количество баллов за экзамен – 22 балла. | |
| **Оценка по дисциплине** | | Оценка по дисциплине выставляется по сумме баллов за текущий контроль и рубежный контроль:   * 85–100 баллов – оценка «отлично»; * 71–84 балла – оценка «хорошо»; * 60–70 баллов – оценка «удовлетворительно»;   менее 60 баллов – оценка «неудовлетворительно» | |

# Фонд оценочных средств

## Паспорт фонда оценочных средств

| № п/п | Индикатор достижения компетенции | Наименование оценочного средства |
| --- | --- | --- |
| 1 | ВПК-1.1. Выбирает необходимый криптографический протокол и выполняет его программную реализацию | * практические задания №1,4,5, 7,8 * контрольные работы. |
| 2 | ВПК-1.2. Выбирает механизм консенсуса, разрабатывает и реализует архитектуру безопасного блокчейн решения | * практические задания №2, 3, 6 * контрольные работы. |

**Практическое задание №1. Алгоритм RSA.**

***Цель работы:*** научиться на практике применять алгоритмы асимметричной криптографии.

***Задача:*** Смоделировать работу алгоритма шифрования RSA

**Практическое задание №2 Поиск nonce для протокола консенсуса. Доказательство работы.**

***Цель работы:*** изучить работу механизмов консенсусов блокчейн систем на примере консенсуса Доказательство работы..

***Задача:*** Смоделировать работу алгоритма Proof-of-Work.

**Практическое задание №3 Построение схемы аутентификации для заданной блокчейн-системы.**

***Цель работы:*** научиться на практике применять протоколы разделения аутентификации.

***Задача:*** Разработать схему аутентификации для авторизации и работы с приложением, в основе которого лежит использование блокчейн системы.

**Практическое задание №4. Распределение ключа по заданному протоколу.**

***Цель работы:*** научиться на практике применять протоколы разделения секрета, основанные на решении различных математических задач.

***Задачи:***

Смоделировать процесс разделения секретного значения между тремя, четырьмя, пятью пользователями с использованием схемы Блекли.

Смоделировать процесс разделения секретного значения между тремя, четырьмя, пятью пользователями с использованием схемы Шамира.

Смоделировать процесс разделения секретного значения между тремя, четырьмя, пятью пользователями с использованием китайской теоремы об остатках.

**Практическое задание №5. Основы реализации протокола с нулевым разглашением знания.**

***Цель работы:*** научиться на практике применять протокол идентификации с нулевым разложением на основе использования схемы Фейге-Фиата-Шамира.

***Задача:*** Смоделировать процесс взаимодействия двух пользователей для их идентификации при использовании схемы Фейге-Фиата-Шамира с нулевым разглашением.

**Практическое задание №6. Основы реализации протокола электронного голосования.**

***Цель работы:*** научиться на практике применять протоколы при анонимном распределении ключей, протоколы электронного голосования на основе использования схемы игры в покер по телефону.

***Задача:*** Смоделировать процесс взаимодействия n пользователей при их взаимодействии в ходе проведения ананимного электронного голосования.

**Практическое задание №7. Основы реализации протокола распределения ключа.**

***Цель работы:*** научиться на практике применять протоколы распределения ключей.

***Задача:*** Разработать и реализовать программу для управления ключами.

**Практическое задание №8. Построение схемы работы оракула для блокчейн-системы.**

***Цель работы:*** научиться на практике применять оракулы для блокчейн систем.

***Задача:*** Разработать и реализовать оракул по передаче в блокчейн систему текущих курсов валют.

**Дополнительный материал для выполнения практических заданий**

**Задачи коллективного разделения секрета**

**Схема Блекли.**

Как известно, система *k* линейно независимых сравнений от *k* неизвестных по простому модулю имеет ровно одно решение.

На этом основана пороговая схема Блекли, созданная в 1979 году. Секрет *m* разделяется между *n* абонентами так, что любая группа, состоящая не менее, чем из *k* абонентов, является разрешенной.

Параметрами схемы являются:

*p* – большое простое число. *p* должно быть больше любого секрета, который предполагается разделять в этой схеме (*p>m*). Тогда *m*Z*p*.

*n* – число долей секрета.

*k* – минимальный размер разрешенной группы.

**Подготовительная фаза:**

Случайным образом раздающий выбирает числа *x*2\*, *x*3\*, … ,*xk*\*Z*p*. Тем самым получена секретная точка Q = (*m*,*x*2\*, *x*3\*, … ,*xk*\*).

**Фаза раздачи секрета:**

Для *i*-го (*i*=1,…,*n*) участника раздающий выбирает случайные равномерно распределенные на Z*p* коэффициенты *a*1*i*, *a*2*i*, *a*3*i*, … , *aki* и вычисляет *bi=a*1*im + a*2*ix*2\*+…+*akixk*\* mod*p*.

После чего раздающий D посылает абоненту P*i* сравнение

*a*1*ix*1*+a*2*ix*2+…+*akixk≡ bi*(mod *p*)

(а, точнее, его коэффициенты) с неизвестными *x*1, *x*2, …, *xk*.

При этом раздающий должен следить за тем, чтобы любые *k* сравнений были линейно независимы.

**Фаза восстановления секрета:**

Собравшись вместе, *k* абонентов могут составить из своих cравнений систему

*a*11*x*1+ *a*21*x*2*+…+ak*1*xk≡b*1(mod *p*)

*a*12*x*1*+ a*22*x*2*+…+ak*2*xk≡b*2(mod *p*)

………………………….

*a*1*kx*1*+ a*2*kx*2*+…+akkxk≡bk*(mod *p*)

решив которую они отыщут точку Q, первая координата которой как раз и будет секретом *m*.

**Пример.**

Построим (3,3) – пороговую схему Блекли. В качестве секрета возьмем m=5, в качестве модуля *p*=11. В качестве секретной точки выберем Q=(*m*=5, *x*2\*=2, *x*3\*=1).

Фаза раздачи:

Вычислим доли секрета для каждого абонента:

Для P1: Выберем*a*11=1, *a*21=1, *a*31=1. Тогда*b*1=1·5+1·2+1·1 mod 11=8.

Для P2: Выберем*a*12=3, *a*22=2, *a*32=7. Тогда*b*2=3·5+2·2+7·1 mod 11=4.

Для P3: Выберем*a*13=8, *a*23=1, *a*33=10. Тогда *b*3=8·5+1·2+10·1 mod 11=8.

Заметим, что после фазы раздачи у каждого из участников оказалось по 4 коэффициента линейного сравнения.

Фаза восстановления:

Участники P1, P2, P3 составляют систему линейных сравнений. У каждого из них есть по одному сравнению. Получившаяся система состоит из трех сравнений и имеет три неизвестных. Если матрица системы невырожденная, то система имеет единственное решение.



Представим эту систему в виде расширенной матрицы и решим методом Гаусса, учитывая, что операции производятся в Z11.

.

Итак, решив систему сравнений, участники нашли единственную точку *x*1=5, *x*2=2, *x*3=1, которая совпадает с точкой Q, и восстановили секрет *m*=5.

Посмотрим, что случится, если свои секреты объединят не три, а два участника. Удастся ли им узнать значение *m*, или хотя бы очертить круг возможных его значений?

Пусть секрет пытаются восстановить участники P1 и P2. Тогда расширенная матрица системы, составленной ими, будет



Таким образом, решение, полученное этими участниками, будет

*m=x*1=10—*x*3mod 11

*x*2=9—7*x*3mod 11

Но тогда *m* может принимать любое значение от 0 до 10, то есть участники P1 и P2, собравшись вместе, не увеличили своих знаний о секрете.

**Схема Шамира**

Идея, на которой основана данная схема, заключается в том, что для интерполяции многочлена степени *k—*1 требуется*k* точек. Если известно меньшее количество точек, то интерполяция будет невозможной.

*p* – большое простое число. *p* должно быть больше любого секрета, который предполагается разделять в этой схеме (*p>m*). Тогда *m*Z*p*.

*n* – число долей секрета.

*k* – минимальный размер разрешенной группы.

**Подготовительная фаза:**

Раздающий выбирает коэффициенты *s*1, *s*2, … ,*sk-*1 Z*p* случайным образом и составляет секретный полином S(*x*) *= m+s*1*x+s*2*x*2+ … *+sk-*1*xk-*1mod*p*

**Раздача секрета:**

Каждому участнику посылается его доля секрета. Долей секрета *i-*го участника является пара чисел (*i*, S(*i*)).

**Восстановление секрета:**

Пусть свои доли секрета объединяют *k* участников с номерами *i*1, *i*2, … ,*ik*. Такая группа участников располагает долями (*i*1,S(*i*1)), (*i*2,S(*i*2)), …, (*ik*,S(*ik*)). Каждая такая доля является точкой многочлена S(*x*), который имеет степень *k—*1. Поэтому, обладая *k* точками этого многочлена, участники могут восстановить коэффициенты многочлена, либо решив систему линейных сравнений относительно неизвестных коэффициентов *m*, *s*1, *s*2, … ,*sk-*1, либо воспользовавшись интерполяционным многочленом Лагранжа:

S(*x*)=

и учтя, что *m=*S(0).

**Пример.**

Построим (3,3)-пороговую схему Шамира. В качестве секрета возьмем *m*=18, в качестве модуля *p*=31.

Подготовительная фаза:

Раздающий выбирает коэффициенты s1=13, s2=6.

Тогда S(*x*)=18+13*x*+6*x*2.

Фаза раздачи:

Доля P1: S(1)=18+13·1+6·1 mod 31=37 mod 31 = 6;

Доля P2: S(2)=18+13·2+6·4 mod 31=68 mod 31 = 6;

Доля P3: S(3)=18+13·3+6·9 mod 31=111 mod 31 =18.

Фаза восстановления:

Участники P1, P2, P3 объединяют свои доли секрета, пользуясь интерполяционным многочленом Лагранжа, и получают

S(x)= mod 31 =

= 3(*x*2*—*5*x+*6)*—*6(*x*2*—*4*x+*3)+9(*x*2*—*3*x*+2) mod 31 = 18*—*18*x*+6*x*2 mod 31 =

= 18+13x+6x2mod 31.

*m*=S(0)=18. Секрет восстановлен.

**Схема на основе Китайской теоремы об остатках.**

Сформулируем теорему, на основе которой можно построить пороговую схему разделения секрета.

**Китайская теорема об остатках (I век до н.э. Сунь-Цзе)**

Пусть *m*1,…, *mk* – попарно простые числа **система сравнений вида



, где *m*1, *m*2, …, *mk* – попарно простые числа, имеет единственное решение

*x*0≡, где *M=*, *Mi*=, .

□

Схема разделения секрета на основе китайской теоремы об остатках выглядит следующим образом:

Пусть*N* – общий секрет.

**Фаза разделения секрета:**

Берем *p*1, *p*2,…, *pn* – различные простые числа.

Часть секрета, выдаваемая *i*-му участнику схемы, есть число *xi*, вычисляемое как *xi≡N*(mod*pi*).

Заметим, что числа *p*1, *p*2,…, *pn* должны быть такими, чтобы произведение любых *k* из них было больше, чем *N*. А это достигается, когда для всех *i* выполняется *pi*>.

Для того, чтобы *k–*1 участников не смогли восстановить секрет без *k*-го участника, необходимо, чтобы *pi*<<.

Итак, относительно чисел *p*1, *p*2,…, *pn* должны выполняться условия:

<*pi*<<.

**Фаза восстановления секрета:**

Собравшись вместе, *k* участников составляют и решают систему сравнений относительно неизвестного *N*:

.

Решив систему, участники получают общий секрет *N*.

**Пример.**

Построим (3,3) – пороговую схему на основе Китайской теоремы об остатках для разделения секрета *N*=549.

Определим область, из которой будем выбирать простые числа.

, . Итак, 8,2<*pi*<<23,4.

Выберем *p*1=11, *p*2=13, *p*3=17.

Фаза раздачи секрета:

*x*1= *N*mod*p*1 = 549 mod 11 = 10;

*x*2=*N* mod *p*2 = 549 mod 13 = 3;

*x*3=*N* mod *p*3 = 549 mod 17 = 5.

Доля P1: (*x*1=10, *p*1=11);

Доля P2: (*x*2=3, *p*2=13);

ДоляP3: (*x*3=5, *p*3=17).

Фаза восстановления секрета:

Участники P1, P2 и P3, составляют систему сравнений



и решают ее по Китайской теореме об остатках:

*N*=10·221·1+3·187·8+5·143·5mod 11·13·17 = 2210+4488+3575 mod 2431 = 2210+2057+1144 mod 2431 = 549.

Действительно, секрет был восстановлен тремя участниками.

Теперь посмотрим, что случится, если секрет захотят восстановить только два участника – например, P1 и P2. Эти участники составят с помощью своих долей секрета систему:



и получат ее решение:

*N* = 10·13·6+3·11·6mod 11·13 = 780+198 mod 143 = 978 mod 143 = 120.

Как видим, получилось совсем другое значение, а не секрет. То есть неразрешенная группа из двух человек не сумела восстановить секрет, пользуясь своими долями.

**Тема Схема идентификации Фейге-Фиата-Шамира**

Схема цифровой подписи и проверки подлинности, разработанная Амосом Фиатом (AmosFiat) и Ади Шамиром (AdiShamir), рассматривается в.УриельФейге (UrielFeige), Фиат и Шамир модифицировали алгоритм, превратив его в доказательство подлинности с нулевым знанием. Это лучшее доказательство подлинности с нулевым знанием.

Перед выдачей любых закрытых ключей арбитр выбирает случайный модуль , n, который является произведением двух больших простых чисел. В реальной жизни длина n должна быть не меньше 512 битов и лучше как можно ближе к 1024 битам. n может общим для группы контролеров. (Использование чисел Блюма (Blum) облегчит вычисления, но не является обязательным для безопасности.)

Для генерации открытого и закрытого ключей Пегги доверенный арбитр выбирает число v, являющееся квадратичным остатком mod n. Другими словами выбирается v так, чтобы уравнение x2 ≡ v (mod n) имело решение, и существовало v-1modn. Это v и будет открытым ключом Пегги. Затем вычисляется наименьшее s, для которого s ≡ sqrt (v-1) (mod n). Это будет закрытый ключ Пегги. Используется следующий протокол идентификации.

1) Пегги выбирает случайное r, меньшее n. Затем она вычисляет x =-r2mod n и посылает x Виктору.

2) Виктор посылает Пегги случайный бит b.

3) Если b = 0, то Пегги посылает Виктору r. Если b = 1, то Пегги посылает Виктору y = r\*s mod n.

4) Если b = 0, Виктор проверяет, что x = -r2mod n, убеждаясь, что Пегги знает значение sqrt(x). Если b = 1, Виктор проверяет, что x = y2\*v mod n, убеждаясь, что Пегги знает значение sqrt(v-1).

Это один этап протокола, называемый аккредитацией. Пегги и Виктор повторяют этот протокол t раз, пока Виктор не убедится, что Пегги знает s. Это протокол "разрезать и выбрать". Если Пегги не знает s, она может подобрать r так, что она сможет обмануть Виктора, если он пошлет ей 0, или она может подобрать r так, что она сможет обмануть Виктора, если он пошлет ей 1 . Она не может сделать одновременно и то, и другое. Вероятность, что ей удастся обмануть Виктора один раз, равна 50 процентам . Вероятность, что ей удастся обмануть его t раз, равна 1/2t.

Виктор может попробовать вскрыть протокол, выдавая себя за Пегги . Он может начать выполнение протокола с с другим контролером, Валерией. На шаге (1) вместо выбора случайного r ему останется просто использовать значение r, которое Пегги использовала в прошлый раз . Однако, вероятность того, что Валерия на шаге (2) выберет то же значение b, которое Виктор использовал в протоколе с Пегги, равна 1/2 . Следовательно, вероятность, что он обманет Валерию, равна 50 процентам . Вероятность, что ему удастся обмануть ее t раз, равна 1/2t.Чтобы этот протокол работал, Пегги никогда не должна использовать r повторно. В противном случае, если Виктор на шаге (2) пошлет Пегги другой случайный бит, то он получит оба ответа Пегги . Тогда даже по одному из них он сможет вычислить s, и для Пегги все закончится.В своих работах, Фейге, Фиат и Шамир показали, как параллельная схема может повысить число аккредитаций на этап и уменьшить взаимодействия Пегги и Виктора.

Сначала, как и в предыдущем примере, генерируется n, произведение двух больших простых чисел. Для ге-

нерации открытого и закрытого ключей Пегги сначала выбирается k различных чисел: v1, v2, . . . vk, где каждое vi является квадратичным остатком mod n. Иными словами, vi выбираются так, чтобы x2 ≡ vi (mod n) имело решение, и существовало vi-1mod n. Строка, v1, v2, . . . vk, служит открытым ключом. Затем вычисляются наименьшие si, для которых si ≡ sqrt (vi-1) (mod n). Строка s1, s2, . . . sk, служит закрытым ключом.

Выполняется следующий протокол:

1) Пегги выбирает случайное r, меньшее n. Затем она вычисляет x =-r2mod n и посылает x Виктору.

2) Виктор посылает Пегги строку из k случайных битов: b1, b2, . . . bk.

3) Пегги вычисляет y = r \*(s1b1\*s2b2K\*k\*bsk)mod n. (Она перемножает вместе значения si, соответствующие bi=1. Если первым битом Виктора будет 1, то s1 войдет в произведение, а если первым битом будет 0, то нет, и т.д.) Она посылает y Виктору.

4) Виктор проверяет, что x = y2\*(v1b1\*v2b2K\*\*kbvk )mod n. (Он перемножает вместе значения vi, основываясь на случайной двоичной строке. Если его первым битом является 1, то v1 войдет в произведение, а если первым битом будет 0, то нет, и т.д.)

Пегги и Виктор повторяют этот протокол t раз, пока Виктор не убедится, что Пегги знает s1, s2, . . . sk. Вероятность, что Пегги удастся обмануть Виктор t раз, равна 1/2kt. Авторы рекомендуют использовать вероятность мошенничества 1/220 и предлагают значения k = 5 и t = 4. Если у вас склонность к мании преследования, увеличьте эти значения.

Пример

Взглянем на работу этого протокола небольших числах . Если n = 35 (два простых числа - 5 и 7), то возможными квадратичными остатками являются:

1: x2 ≡ 1 (mod 35) имеет решения: x = 1, 6, 29, 34.

4: x2 ≡ 4 (mod 35) имеет решения: x = 2, 12, 23, 33.

9: x2 ≡ 9 (mod 35) имеет решения: x = 3, 17, 18, 32.

11: x2 ≡ 11 (mod 35) имеет решения: x = 9, 16, 19, 26.

14: x2 ≡ 14 (mod 35) имеет решения: x = 7, 28.

15: x2 ≡ 15 (mod 35) имеет решения: x = 15, 20.

16: x2 ≡ 16 (mod 35) имеет решения: x = 4, 11, 24, 31.

21: x2 ≡ 21 (mod 35) имеет решения: x = 14, 21.

25: x2 ≡ 25 (mod 35) имеет решения: x = 5, 30.

29: x2 ≡ 29 (mod 35) имеет решения: x = 8, 13, 22, 27.

30: x2 ≡ 30 (mod 35) имеет решения: x = 10, 25.

Обратными значениями (mod 35) и их квадратными корнями являются:

v -1 v s=sqrt(v-1)

1 1 1

4 9 3

9 4 2

11 16 416 11 9

29 29 8

Обратите внимание, что у чисел 14, 15, 21, 25 и 30 нет обратных значений mod 35, так как они не взаимнопросты с 35. Это имеет смысл, так как должно быть (5 - 1) \* (7 - 1)/4 квадратичных остатков mod 35, взаимнопростых с 35: НОД(x, 35) = 1.

Итак, Пегги получает открытый ключ, состоящий из k = 4 значений: {4,11,16,29}. Соответствующим закрытым ключом является {3,4,9,8}. Вот один этап протокола.

1) Пегги выбирает случайное r=16, вычисляет 162mod 35 = 11 и посылает его Виктору.

2) Виктор посылает Пегги строку случайных битов: {1, 1, 0, 1}

3) Пегги вычисляет 16\*(31\*41\*90\*81) mod 35 = 31 и посылает его Виктору.

4) Виктор проверяет, что 312\*(41\*111\*160\*291) mod 35 =11.

Пегги и Виктор повторяют этот протокол t раз, каждый раз с новым случайным r, пока Виктор будет убежден.

Небольшие числа, подобные использованным в примере, не обеспечивают реальной безопасности . Но когдадлина n равна 512 и более битам, Виктор не сможет узнать о закрытом ключе Пегги ничего кроме того факта, что Пегги действительно знает его.

**Критерии оценки:**

* оценка «отлично» выставляется студенту, если практическая работа выполнена в срок, студент показывает глубокое знание изучаемого вопроса, может ответить на вопросы, связанные с ходом выполнения работы, знает и умеет применить на практике приемы, которые использовались в работе, умеет экстраполировать изученный метод на другие задачи.
* оценка «хорошо» выставляется студенту, если работа выполнена в срок, студент показывает знание основных вопросов изучаемого метода, может ответить на вопросы, связанные с ходом выполнения работы, знает и умеет применить на практике основные алгоритмы, которые использовались в работе для достижения поставленной цели;
* оценка «удовлетворительно» выставляется студенту, если работа выполнена в срок, студент может ответить на вопросы, связанные с ходом выполнения работы, знает основные алгоритмы, которые использовались в работе для достижения поставленной цели;
* оценка «неудовлетворительно» выставляется в том случае, если не выполнено ни одно из требований для вышеперечисленных критериев оценки.

**Пример вопросов для проведения контрольных работ:**

Контрольная работа составляется из пула вопросов случайным выборов 10 из них.

1. Что такое генезис блок?
2. Что означает поле gaslimit в структуре генезис блока?
3. Что означает поле difficulty в структуре генезис блока?
4. Какие поля могут присутствовать в генезис блоке?
5. Для чего в команде запуска geth прописывается параметр dev?
6. Какой параметр позволяет работать с geth в консольном режиме?
7. Какой параметр позволяет присоединиться к уже поднятой ноде?
8. Что означает параметр networkid, используемый при запуске geth?
9. Команда для создания нового адреса в сети
10. Команды для запуска и остановки майнера
11. Какой командой можно назначить пользователя, у которого пополняется счет в процессе майнинга?
12. Как просмотреть баланс пользователя?
13. Команда для разблокировки пользователя
14. Эфир (Ether) в сети Ethereum — это:
15. Что такое смарт-контракт?
16. Газ (gas) в сети Ethereum — это:
17. Где берут газ (gas) для проведения транзакций? (Несколько вариантов ответа)
18. На каком языке программирования ведется разработка смарт-контрактов?
19. Какие типы переменных присутствуют в языке программирования Solidity?
20. В чем особенность view функций в языке Solidity?
21. Как смарт-контракты идентифицируются в сети?
22. От чего зависит количество потребляемого газа?
23. В чем особенность storage памяти?
24. В чем особенность memory памяти?
25. Какие платформы для создания блокчейн-решений существуют?
26. За какой промежуток времени (в среднем показателе) создается блок в Bitcoin?
27. Что такое Корень Меркла в биткоине?
28. Что значит, что блокчейн-технология является децентрализованной?
29. Что необходимо знать, чтобы проверить подпись транзакции
30. Что необходимо знать, чтобы проверить подпись блока?
31. За счет чего достигается защита от транзакций с двойным расходом?
32. Назовите основные характеристики технологии блокчейн Bitcoin.
33. Назовите основную задачу платформы Ethereum.
34. Назовите основные задачи майнеров?

**Критерии оценки:**

* оценка «отлично» выставляется в случае, если все задания выполнены правильно и в полном объеме;
* оценка «хорошо» выставляется в том случае, если выполнены все задания, но при описании и вычислениях допущены неточности или незначительные ошибки;
* оценка «удовлетворительно» выставляется в том случае, если задания выполнены не в полном объеме, также в том случае, если при выполнения задания допущены грубые ошибки;
* оценка «неудовлетворительно» выставляется в том случае, если не выполнено ни одно условие.

**Пример задания для демонстрационного экзамена**

Есть объект движимого имущества.

В нашей системе учтено, что собственником имущества является какой-то адрес.

В системе должен быть администратор, который регистрирует объекты недвижимого имущества. В системе должна быть предусмотрена функция смены ролей в системе.

Параметры объекта движимого имущества, которые должны отображаться:

- собственник

- тип объекта (мототранспорт, легковой транспорт, грузовой транспорт, другое)

- обременения (в залоге или нет)

- год выпуска

- государственный номер

Объект движимого имущества можно продать, подарить, сдать в аренду.

Продажа:

Собственник движимого имущества создает предложение продажи этого имущества. Покупатель должен перевести средства, продавец должен подтвердить (забрать) средства и тогда собственником становится тот, кто перевел средства.

При создании продажи должны указываться:

- объект продажи (что именно продается)

- стоимость продажи

- срок продажи (в течении какого периода смарт-контракт актуален)

Должны быть реализованы:

- возможность отмены продажи

- возможность возврата средств отправителю, если продавец отказывается от продажи

- возможность возврата средств отправителю, если продавец не подтвердил и закончился срок продажи

- механизм подтверждения получения средств продавцом.

Дарение:

Собственник указывает нового владельца объекта движимого имущества. Процедура дарения завершается при подтверждении новым владельцем, с целью исключения ошибки при указании нового владельца.

Аренда:

Собственник может сдать свой объект движимого имущества в аренду на определенный срок, получив при этом определенную сумму средств.

Создание:

- указывается объект аренды

- указывается нужная сумма

- указывается срок аренды

Арендодатель переводит средства по конкретному объекту движимого имущества, собственник подтверждает, что получил эти средства, после подтверждения начинается отсчет срока аренды.

Собственник всегда может отменить свое предложение, пока он не подтвердил получение средств.

Арендодатель всегда может отозвать свои средства, пока собственник не подтвердил их получение.

В рамках второго модуля должны быть продемонстрированы навыки компиляции и деплоя контрактов.

Задачи второго модуля должны быть спланированы по времени модуля и распределены между участниками команды. При выполнении заданий второго модуля необходимо вести документирование кода. Должна быть дана инструкция по установке, запуску и использования решения.

### **Примерный сценарий для проведения оценивания практикоориентированного экзамена**

**Демонстрация купля-продажа**

Продемонстрировать работу созданного приложения. При этом показывать отображение записей в блокчейн-системе. Для отображения изменения информации допускается использовать любые визуализирующие надстройки.

Проделать нижеприведенные действия сначала через GUI. Потом через консоль.

Запустить приложение от лица администратора системы. Отобразить счет администратора. Добавить от лица администратора новый объект одному из пользователей.

Запустить приложение от лица первого собственника. Показать счет первого собственника и его недвижимое имущество. Выставить жилье на продажу.

Запустить приложение от лица второго собственника. Показать счет второго собственника и его недвижимое имущество. Выставить жилье на продажу. Просмотреть объявления о продаже. Купить жилье первого собственника.

Запустить приложение от лица первого собственника. Подтвердить получение денег за продажу. Показать изменение баланса. Показать недвижимость первого пользователя. Купить жилье второго собственника.

Запустить приложение от лица второго собственника. Проверить, что купленная квартира перешла в его собственность. Показать изменение баланса. Посмотреть предложение о покупке квартиры от первого собственника. Снять квартиру с продажи (не подтверждать получение денег). Показать все квартиры собственника

Запустить приложение от лица первого собственника. Показать счет первого собственника и его недвижимое имущество.

Запустить приложение от лица администратора системы. Добавить первому собственнику новый объект.

Запустить приложение от лица администратора системы. Добавить от лица администратора новый объект одному из пользователей.

Запустить приложение от лица первого собственника. Показать его недвижимое имущество.

**Демонстрация аренда**

Продемонстрировать работу созданного приложения. При этом показывать отображение записей в блокчейн-системе. Для отображения изменения информации допускается использовать любые визуализирующие надстройки.

Проделать нижеприведенные действия сначала через GUI. Потом через консоль.

Запустить приложение от лица администратора системы. Отобразить счет администратора. Добавить от лица администратора новый объект одному из пользователей.

Запустить приложение от лица первого собственника. Показать счет первого собственника и его недвижимое имущество. Выставить жилье на аренду.

Запустить приложение от лица второго собственника. Показать счет второго собственника и его недвижимое имущество. Выставить жилье на аренду. Просмотреть объявления об аренде. Взять в аренду жилье первого собственника.

Запустить приложение от лица первого собственника. Подтвердить получение денег за аренду. Показать изменение баланса. Показать недвижимость первого пользователя. Взять в аренду жилье второго собственника.

Запустить приложение от лица второго собственника. Показать изменение баланса. Посмотреть предложение об аренде квартиры от первого собственника. Снять квартиру с аренды (не подтверждать получение денег). Показать все квартиры собственника

Запустить приложение от лица первого собственника. Показать счет первого собственника и его недвижимое имущество.

**Демонстрация дарение**

Запустить приложение от лица администратора системы. Добавить первому собственнику новый объект.

Запустить приложение от лица администратора системы. Добавить от лица администратора новый объект одному из пользователей.

Запустить приложение от лица первого собственника. Показать его недвижимое имущество. Подарить жилье второму собственнику.

Запустить приложение от лица второго собственника. Показать его недвижимое имущество. Подарить жилье первому собственнику. Просмотреть уведомления о дарении. Принять в дар жилье первого собственника. Отобразить все имущество второго собственника.

Запустить приложение от лица первого собственника. Отказаться от предложения дарения. Показать недвижимость первого пользователя.

Запустить приложение от лица второго собственника. Показать все квартиры собственника.

**Критерии оценки:**

За каждый выполненный пункт при проверке задания выставляется 1 балл. Максимальное количество баллов – 40. Минимальное количество баллов – 22.