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

**Безопасность решений на основе использования блокчейн-технологий**

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](#_Toc64926090)

[II. Место дисциплины в структуре образовательной программы 4](#_Toc64926091)

[III. Требования к результатам освоения дисциплины 5](#_Toc64926092)

[IV. Содержание и структура дисциплины 6](#_Toc64926093)

[4.1. Содержание дисциплины, структурированное по темам 6](#_Toc64926094)

[4.2. План внеаудиторной самостоятельной работы 8](#_Toc64926095)

[4.3. Содержание учебного материала 10](#_Toc64926096)

[V. Образовательные технологии 11](#_Toc64926097)

[VI. Учебно-методическое обеспечение дисциплины 11](#_Toc64926098)

[6.1. Основная литература 11](#_Toc64926099)

[6.2. Дополнительная литература 11](#_Toc64926100)

[VII. Материально-техническое обеспечение дисциплины 11](#_Toc64926101)

[VIII. Методические указания для обучающихся по освоению дисциплины 12](#_Toc64926102)

[IX. Учебная карта дисциплины 13](#_Toc64926103)

[X. Фонд оценочных средств 14](#_Toc64926104)

[10.1. Паспорт фонда оценочных средств 14](#_Toc64926105)

[10.2 Практические задания 14](#_Toc64926106)

[10.3 Контрольные работы по модулям 1 и 2 19](#_Toc64926107)

# Цели и задачи освоения дисциплины

Цели освоения дисциплины:

* формирование у студентов базовых знаний в области безопасности решений на основе блокчейн – технологий, а также в области разработки смарт-контрактов.

Задачи освоения дисциплины:

* изучение типов уязвимостей в блокчейн-системах;
* изучение уязвимостей в различных блокчейн-платформах;
* рассмотрение методов построения смарт-контрактов;
* рассмотрение основных уязвимостей клиентских приложений для работы с блокчейн-системами.

# Место дисциплины в структуре образовательной программы

Дисциплина относится к модулю вариативных 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 при освоении следующих элементов образовательной программы:

* 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-1.3. Формулирует перечень возможных угроз безопасности, осуществляет проверку основных сценариев тестирования блокчейн-решений | Выявление угроз безопасности информации в автоматизированных системах |

# Содержание и структура дисциплины

Трудоёмкость дисциплины составляет 5 зачётных единиц, 180 часов.

Форма промежуточной аттестации: дифференцированный зачёт

## 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.** «Уязвимости в блокчейн-системах» | | | | | | | |
| 1 | Тема 1. Типы уязвимостей в блокчейн-системах | 3 | 2 | 2 | - | 12 | * работа на лекционных занятиях по модулю 1 (дискуссия); * практические занятия по модулю 1 (защита практического задания №1 «Рассмотрение кейсов по уязвимости блокчейн-систем»). |
| 2 | Тема 2. Уязвимости современных блокчейн-платформ. На примере платформ Ethereum, Hyper Ledger, EOS, NEO. | 3 | 4 | 4 | - | 18 | * практические занятия по модулю 1 (защита практического задания №2 «Разработка схем по устранению существующих уязвимостей блокчейн систем.»). |
| 3 | Тема 3. Обзор потенциальных кибератак на криптовалюты. Стоимость проводимых атак. | 3 | 2 | 2 | - | 12 | ‒ практические занятия по модулю 1 (защита практического задания №3 «Разработка стратегии защиты от потенциальных атак.»). |
| **Модуль 2.** «Разработка и тестирование смарт-контрактов» | | | | | | | |
| 4 | Тема 4. Методы построения смарт-контрактов. Смарт-контракт для системы Ethereum. Язык Solidity. | 3 | 4 | 4 | - | 17 | * практические занятия по модулю 2 (защита практического задания №4 «Создание смарт-контракта на заданную тему», защита практического задания №5 «Создание клиентского приложения для работы смарт-контракта»). |
| 5 | Тема 5. Основные уязвимости смарт-контрактов Ethereum. Методы тестирования логики работы смарт-контрактов Ethereum. | 3 | 4 | 4 | - | 17 | * практические занятия по модулю 2 (защита практического задания №6 «Покрытие смарт-контракта тестами»). |
| 6 | Тема 6. Основные уязвимости клиентского приложения для работы с блокчейн-системой. | 3 | 2 | 2 | - | 17 | * практические занятия по модулю 2 (защита практического задания №7 «Покрытие клиентского приложения тестами»). |
| **Итого часов** | | 3 | 18 | 18 | 0 | 144 | – |

## План внеаудиторной самостоятельной работы

| № п/п | Темы дисциплины | Семестр | Вид самостоятельной работы | Сроки выполнения (нед.) | Затраты времени (часы) | Учебно-методическое обеспечение |
| --- | --- | --- | --- | --- | --- | --- |
| **Модуль 1.** «Уязвимости в блокчейн-системах» | | | | | | |
| 1 | Тема 1. Типы уязвимостей в блокчейн-системах | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №1. | 1–2 | 12 | Задание к практической работе №1, основная и дополнительная литература |
| 2 | Тема 2. Уязвимости современных блокчейн-платформ. На примере платформ Ethereum, Hyper Ledger, EOS, NEO. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №2. | 3–5 | 18 | Задание к практической работе №2, основная и дополнительная литература |
| 3 | Тема 3. Обзор потенциальных кибератак на криптовалюты. Стоимость проводимых атак. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №3. | 6–7 | 12 | Задание к практической работе №3, основная и дополнительная литература |
| **Модуль 2.** «Разработка и тестирование смарт-контрактов» | | | | | | |
| 4 | Тема 4. Методы построения смарт-контрактов. Смарт-контракт для системы Ethereum. Язык Solidity. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №4; * выполнение практического задания №5. | 8-13 | 17 | Задание к практическим работам №4-5, основная и дополнительная литература |
| 5 | Тема 5. Основные уязвимости смарт-контрактов Ethereum. Методы тестирования логики работы смарт-контрактов Ethereum. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №6. | 14-16 | 17 | Задание к практической работе №6, основная и дополнительная литература |
| 6 | Тема 6. Основные уязвимости клиентского приложения для работы с блокчейн-системой. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №7. | 17-18 | 17 | Задание к практической работе №7, основная и дополнительная литература |
| **Общая трудоёмкость самостоятельной работы по дисциплине** | | | | | 144 | – |

## Содержание учебного материала

**Модуль 1. «Уязвимости в блокчейн-системах»**

**4.3.1. Типы уязвимостей в блокчейн-системах.** Угрозы и уязвимости ИС. Классификация угроз безопасности ИС. Методы оценивания угроз безопасности КС.

**4.3.2. Уязвимости современных блокчейн-платформ. На примере платформ Ethereum, Hyper Ledger, EOS, NEO.** Обзор платформ. Назначение платформ. Преимущества и недостатки платформ.

**4.3.3. Обзор потенциальных кибератак на криптовалюты. Стоимость проводимых атак.** Обзор криптовалют. Обзор уязвимостей криптовалют. Обзор кибератак.

**Модуль 2. «Разработка и тестирование смарт-контрактов»**

**4.3.4. Методы построения смарт-контрактов. Смарт-контракт для системы Ethereum. Язык Solidity.**

Синтаксис языка Solidity. Разработка смарт-контракта. Развертывание смарт-контракта в сети Ethereum.

**4.3.5. Основные уязвимости смарт-контрактов Ethereum. Методы тестирования логики работы смарт-контрактов Ethereum.**

**4.3.6. Основные уязвимости клиентского приложения для работы с блокчейн-системой.**

Перечень тем практических занятий

| №  п/п | Тема практического занятия | Количество часов |
| --- | --- | --- |
| **Модуль 1. Уязвимости в блокчейн-системах** | | |
| 1 | Практическое задание №1 «Рассмотрение кейсов по уязвимости блокчейн-систем». | 2 |
| 2 | Практическое задание №2 «Разработка схем по устранению существующих уязвимостей блокчейн-систем». | 2 |
| 3 | Практическое задание №3 «Разработка стратегии защиты от потенциальных атак». | 2 |
| 4 | Контрольная работа по модулю 1 | 2 |
| **Модуль 2. Разработка и тестирование смарт-контрактов** | | |
| 5 | Практическое задание №4 «Создание смарт-контракта на заданную тему». | 2 |
| 6 | Практическое задание №5 «Создание клиентского приложения для работы смарт-контракта». | 2 |
| 7 | Практическое задание №6 «Покрытие смарт-контракта тестами». | 2 |
| 8 | Практическое задание №7 «Покрытие клиентского приложения тестами». | 2 |
| 9 | Контрольная работа по модулю 2 | 2 |
| **Всего часов** | | **18** |

# 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 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. Лекционные занятия и другие формы контактной работы обучающихся с преподавателем могут проводиться с использованием платформы Microsoft Teams, OneDrive и 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 отчеты к практическим заданиям, 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. Сингхал Б., Блокчейн. Руководство для начинающих разработчиков: Пер. с англ. / Г. Дамеджа, П.С. Панда. — СПб.: БХВ – Петербург, 2020. — 288 с.: ил.

## Дополнительная литература

2.  S. Liu, P. Viotti, C. Cachin, V. Qu´ema, and M. Vukolic, “Xft: Practical fault tolerance beyond crashes.” in 12th USENIX Symposium on Operating Systems Design and Implementation, Savannah, GA, Nov. 2016, pp. 485–500.

3.  M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, “On bitcoin and red balloons,” in Proceedings of the 13th ACM Conference on Electronic Commerce, ser. EC ’12. New York, NY: ACM, Jun. 2012, pp. 56–73

4. S. Athey, I. Parashkevov, V. Sarukkai, and J. Xia, “Bitcoin pricing, adoption, and usage: Theory and evidence,” Stanford Institute for Economic Policy Research, Tech. Rep. Working Paper No. 3469, Aug. 2016.

5. A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, “Is bitcoin a decentralized currency?” IEEE Security Privacy, vol. 12, no. 3, pp. 54–60, May 2014.

6.  I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable (revised selected papers),” in Financial Cryptography and Data Security: 18th International Conference, Christ Church, Barbados, Mar. 2014, pp. 436–454.

7.  O. Ersoy, Z. Ren, Z. Erkin, and R. L. Lagendijk, “Information propagation on permissionless blockchains,” arXiv preprint arXiv:1712.07564, 2017.

# 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, Open Office.

# 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, Microsoft Teams).

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, осуществляется разбор практических заданий.

Самостоятельная работа студентов включает в себя подготовку к лекционным, практическим занятиям, выполнение практических заданий. 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.

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, семестр 3, очная форма обучения

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Виды контрольных мероприятий  (наименования оценочных средств) | Количество баллов | |
| Текущий контроль | Рубежный контроль |
| Модуль 1. Уязвимости в блокчейн-системах | | | |
| 1 | Практическое задание №1 «Рассмотрение кейсов по уязвимости блокчейн-систем». | 5 | - |
| 3 | Практическое задание №2 «Разработка схем по устранению существующих уязвимостей блокчейн-систем». | 9 | - |
| 4 | Практическое задание №3 «Разработка стратегии защиты от потенциальных атак». | 14 | - |
| 5 | Контрольная работа по модулю 1 | - | 10 |
| Модуль 2. Разработка и тестирование смарт-контрактов | | | |
| 5 | Практическое задание №4 «Создание смарт-контракта на заданную тему». | 13 | - |
| 6 | Практическое задание №5 «Создание клиентского приложения для работы смарт-контракта». | 10 | - |
| 7 | Практическое задание №6 «Покрытие смарт-контракта тестами». | 15 | - |
| 8 | Практическое задание №7 «Покрытие клиентского приложения тестами». | 14 | - |
|  | Контрольная работа по модулю 2 | - | 10 |
| **Всего** | | 80 | 20 |
| Бонусные баллы | | Бонусные баллы не предусмотрены | |
| **Промежуточная аттестация  в форме дифференцированного зачёта** | | 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-1.3. Формулирует перечень возможных угроз безопасности, осуществляет проверку основных сценариев тестирования блокчейн-решений | * практические задания №1-4. * контрольные работы. |

10.2 Практические задания

**Практическое задание №1.**

**«Рассмотрение кейсов по уязвимости блокчейн-систем»**

Задание:

В рамках данной практической работы необходимо выбрать и рассмотреть на предмет уязвимостей одну из известных платформ (Ethereum, NEO, EOS.IO, Hyper Ledger и т.д.).

Критерии оценки выполнения практической работы:

**4-5 баллов** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, а также при защите ответил на все вопросы преподавателя;

**2-3 балла** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, и в процессе защиты продемонстрировал наличие достаточных теоретических знаний в объеме содержания учебной дисциплины, относящейся к данной теме.

**1 балл** – выставляется студенту, если он не своевременно сдал практическую работу, способен ответить на вопросы, касающиеся теоретической составляющей в объеме содержания данной работы;

**0 баллов** – выставляется студенту в случае, если он не сделал и не ответил ни на один вопрос преподавателя.

**Практическое задание №2.**

**«Разработка схем по устранению существующих уязвимостей блокчейн-систем».**

Задание:

Необходимо разработать алгоритм устранения уязвимостей платформы, рассмотренной в предыдущей работе.

Критерии оценки выполнения практической работы:

**8-9 баллов** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, а также при защите ответил на все вопросы преподавателя;

**6-7 балла** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, и в процессе защиты продемонстрировал наличие достаточных теоретических знаний в объеме содержания учебной дисциплины, относящейся к данной теме.

**1-5 баллов** – выставляется студенту, если он не своевременно сдал практическую работу, способен ответить на вопросы, касающиеся теоретической составляющей в объеме содержания данной работы;

**0 баллов** – выставляется студенту в случае, если он не сделал и не ответил ни на один вопрос преподавателя.

**Практическое задание №3.**

**Разработка стратегии защиты от потенциальных атак**

Задание:

Необходимо рассмотреть возможные уязвимости и продумать алгоритм по исключению их появления.

Критерии оценки выполнения практической работы:

**10-14 баллов** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, а также при защите ответил на все вопросы преподавателя;

**5-7 балла** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, и в процессе защиты продемонстрировал наличие достаточных теоретических знаний в объеме содержания учебной дисциплины, относящейся к данной теме.

**1-4 баллов** – выставляется студенту, если он не своевременно сдал практическую работу, способен ответить на вопросы, касающиеся теоретической составляющей в объеме содержания данной работы;

**0 баллов** – выставляется студенту в случае, если он не сделал и не ответил ни на один вопрос преподавателя.

**Практическое задание №4.**

**Создание смарт-контракта на заданную тему**

Критерии оценки выполнения практической работы:

**11-13 баллов** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, а также при защите ответил на все вопросы преподавателя;

**6-10 балла** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, и в процессе защиты продемонстрировал наличие достаточных теоретических знаний в объеме содержания учебной дисциплины, относящейся к данной теме.

**1-5 баллов** – выставляется студенту, если он не своевременно сдал практическую работу, способен ответить на вопросы, касающиеся теоретической составляющей в объеме содержания данной работы;

**0 баллов** – выставляется студенту в случае, если он не сделал и не ответил ни на один вопрос преподавателя.

**Практическое задание №5.**

**Создание клиентского приложения для работы смарт-контракта**

Задание:

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.

Критерии оценки выполнения практической работы:

**9-10 баллов** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, а также при защите ответил на все вопросы преподавателя;

**7-8 баллов** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, и в процессе защиты продемонстрировал наличие достаточных теоретических знаний в объеме содержания учебной дисциплины, относящейся к данной теме.

**1-6 баллов** – выставляется студенту, если он не своевременно сдал практическую работу, способен ответить на вопросы, касающиеся теоретической составляющей в объеме содержания данной работы;

**0 баллов** – выставляется студенту в случае, если он не сделал и не ответил ни на один вопрос преподавателя.

**Практическое задание №6.**

**Покрытие смарт-контракта тестами**

Критерии оценки выполнения практической работы:

**11-15 баллов** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, а также при защите ответил на все вопросы преподавателя;

**7-10 балла** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, и в процессе защиты продемонстрировал наличие достаточных теоретических знаний в объеме содержания учебной дисциплины, относящейся к данной теме.

**1-6 баллов** – выставляется студенту, если он не своевременно сдал практическую работу, способен ответить на вопросы, касающиеся теоретической составляющей в объеме содержания данной работы;

**0 баллов** – выставляется студенту в случае, если он не сделал и не ответил ни на один вопрос преподавателя.

**Практическое задание №7.**

**Покрытие клиентского приложения тестами**

Критерии оценки выполнения практической работы:

**10-14 баллов** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, а также при защите ответил на все вопросы преподавателя;

**5-7 балла** – выставляется студенту, если он своевременно и полностью верно сделал практическую работу, и в процессе защиты продемонстрировал наличие достаточных теоретических знаний в объеме содержания учебной дисциплины, относящейся к данной теме.

**1-4 баллов** – выставляется студенту, если он не своевременно сдал практическую работу, способен ответить на вопросы, касающиеся теоретической составляющей в объеме содержания данной работы;

**0 баллов** – выставляется студенту в случае, если он не сделал и не ответил ни на один вопрос преподавателя.

10.3 Контрольные работы по модулям 1 и 2

Контрольные работы предназначены для проведения рубежного контроля по модулю 1 и модулю 2 и позволяют оценить уровень сформированных знаний в рамках, формируемых модулями дисциплины компетенций, в том числе в ходе самостоятельной работы обучающегося. Ниже приводятся вопросы, предлагаемые обучающимся в ходе выполнения контрольных работ. На каждой контрольной работе обучающемуся предлагается выбрать один или несколько вариантов ответа на каждый вопрос.

**Модуль 1.**« Уязвимости в блокчейн-системах»

Вопрос 1

Назовите основные характеристики блокчейна.

Ответ:

1. технология криптозащиты
2. **учетный журнал**
3. **строго хронологический порядок записей**
4. система сбора и хранения данных

Вопрос 2

Что такое биткоин?

Ответ:

1. криптоключ
2. **цифровой актив**
3. тип кредитной карты
4. **криптовалюта**

Вопрос 3

В каких случаях можно использовать биткоин?

Ответ:

1. **для хранения ценностей**
2. **для совершения электронных оплат**
3. для пополнения бумажных счетов
4. **для покупки услуг**

Вопрос 4

Какой из примеров можно отнести к одноранговому типу общения?

Ответ:

1. онлайн отправка денег другому лицу
2. **отправка письма через интернет другому лицу**
3. перевод денег с помощью организации-посредника
4. отправка письма через почтовое отделение

Вопрос 5

Что такое блокчейн?

Ответ:

1. глобальная сеть с тысячами компьютеров
2. **особо децентрализованный учетный журнал**
3. **ключевая технология, содержащая децентрализованную запись транзакций**
4. централизованная база данных, подтверждающая проведение сделки

Вопрос 6

Назовите основные задачи майнеров?

Ответ:

1. **обработка и подтверждение транзакций**
2. **решение криптографических задач**
3. децентрализованное размещение данных по каждой сделке
4. **создание цепи записей, которые формируют учетный журнал биткойн**

Вопрос 7

Что такое хэш?

Ответ:

1. криптографически зашифрованная сделка
2. **цифровой отпечаток определенного набора данных**
3. децентрализованное разрешение криптографических задач
4. **объем данных в алфавитно-цифровом формате определенной длины**

Вопрос 8

С какой периодичностью добавляются новые блоки со всеми новыми транзакциями в блокчейн?

Ответ:

1. по мере обработки майнерами
2. **каждые десять минут**
3. раз в сутки
4. после 100% заполнения нового блока

Вопрос 9

Назовите вид хеш-функции, которая используется в Биткойн.

Ответ:

1. **SHA256**
2. HAS265
3. SAH256
4. SHA265

Вопрос 10

Каким образом подтверждается сделка в сети биткоин между людьми?

Ответ:

1. банком
2. централизованным хранилищем
3. клиринговой организацией
4. **технологией блокчейн**

**Модуль 2.**«Разработка и тестирование смарт-контрактов»

Вопрос 1

какие ограничения есть у технологии блокчейн?

Ответ:

1. большое количество реализованных проектов
2. **ограниченный объем технических знаний**
3. **неизменяемость записей**
4. **масштабируемость**

Вопрос 2

Что такое псевдоанонимность биткоина?

**Ответ:**

1. каждая сделка с биткоинами может иметь отдельный адрес
2. сделка проводится только получения согласия майнеров
3. **адрес биткоина является идентификатором владельца**
4. сделка с биткоинами подтверждается личным ключом

Вопрос 3

Назовите основные характеристики блокчейна.

Ответ:

1. **является книгой учета хронологически упорядоченных постоянных записей**
2. записи в блокчейне могут быть изменены
3. **может быть использован в других технологиях, кроме Биткоина**
4. обладает анонимностью

Вопрос 4

Назовите основные характеристики Биткоин Кэш.

Ответ:

1. **криптовалюта, появившаяся из-за "принудительного ветвления" в блокчейн Биткоин**
2. это Биткоин
3. блок имеет ограничение до 1 Мб
4. **использует протокол, который ограничивает размер блока 8-ю Мб**

Вопрос 5

Как обозначается Биткоин Кэш?

Ответ:

1. BTC
2. **BCH**
3. **ВСС**
4. **XBC**

Вопрос 6

Что такое Halving?

Ответ:

1. четко ограниченная поставка биткоинов
2. вознаграждение за обработку транзакции увеличивается на увеличение объема блока
3. **каждые четыре года стоимость обработки 210,000 блоков в биткоинах урезается наполовину**
4. вынесение цифровой подписи во внешний блок

Вопрос 7

Какой вид кошелька позволяет хранить личные ключи off-line?

Ответ:

1. мобильный кошелек
2. **аппаратный кошелек**
3. веб-кошелек

Вопрос 8

Как называется хранение, которое осуществляется на устройстве, подключенном к Интернету?

Ответ:

1. холодное хранение
2. **горячее хранение**
3. мобильное хранение
4. веб-хранение

Вопрос 9

Назовите основные функции кошелька криптовалют.

Ответ:

1. **получение**
2. **отправка**
3. **хранение**
4. обмен

Вопрос 10

Что обозначает sweep?

Ответ:

1. холодное хранение биткойнов
2. место хранения личного ключа
3. **импорт биткойнов в реальный кошелек**
4. предоставление публичного доступа к личной сети