Автономная некоммерческая организация высшего образования
«Университет при Межпарламентской Ассамблее ЕврАзЭС»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Введение в криптовалюту

(наименование дисциплины)

Направление подготовки 38.03.05 Бизнес-информатика

Квалификация выпускника Бакалавр

Направленность (профиль) Бизнес-информатика, технология блокчейн - криптовалюта

2022 г.

1. Место дисциплины в структуре образовательной программы, входные требования для освоения дисциплины (при необходимости)

Дисциплина «Введение в криптовалюту» относится к дисциплинам обязательной части Блока 1 «Дисциплины (модули)» программы бакалавриата.

2. Объем дисциплины в зачетных единицах

Объем дисциплины составляет 8 зачетных единиц.

3. Содержание дисциплины, структурированное по темам (разделам)

Раздел 1. Технологии криптовалюты и децентрализация биткойна.

Тема 1.1. Биткойн и альтернативные криптовалюты.

Криптографические хэш-функции. Хеш-указатели и структуры данных. Цифровые подписи и требования к ним. Открытые ключи как идентификаторы личности. Централизация против децентрализации криптовалюты, распределенный консенсус. Консенсус без идентификации: блокчейн.

Тема 1.2. Создание электронного кошелька и работа с ним. Сделки с битконом.

Рассказать о Blockchain.info. Механизмы стимулирования, использующиеся в биткоин.

Тема 1.3. Транзакции, хранение и использование криптовалюты.

Журнал (реестр) в режиме Append-Only. Децентрализованная согласованность. Проверка подлинности транзакций майнерами. Скрипты Биткоина. Приложения из скриптов Биткоина. Структура блока Биткоина. Сеть Биткоина. Присоединение к пиринговой сети Биткоина. Ограничения и улучшения. Пропускные ограничения Биткоина. Хранение биткоинов. Горячее и холодное хранилища. Разделение и распространение ключей. Онлайн-кошельки и обменные биржи. Платежные сервисы. Комиссионные за транзакции. Обмен криптовалют.

Раздел 2. Особенности генерации (майнинга) и основы анонимности.

Тема 2.1 Динамика и аппаратное обеспечение майнинга.

Задача биткойн-майнеров. Процесс поиска достоверного блока. Динамика сложности майнинга. Соотношение времени, затрачиваемого на создание блока, и сложности. Аппаратное обеспечение майнинга. Углубленная схема SHA-256 (безопасный алгоритм хеширования). Энергопотребление и экология. Пулы (объединение, совокупность) совместного майнинга. Неопределенность майнинга. Стимулы и стратегии майнинга. Анонимная электронная валюта на основе слепых подписей. Как лишить Биткойн анонимности. Микширование (смешивание). Алгоритм объединения монет. Tor (система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания) и Шелковый путь.

Тема 2.2. Исследование криптовалюты для инвестирования.

Криптопортфель и его назначение. Экспертное мнение Джона Маккафи. Проект ICO.

Тема 2.3. Система инвестирования – критерий при выборе криптовалюты.

Краткосрочное и долгосрочное инвестирование в электронную денежную единицу. Соотношение риск/прибыль, снижение цены/рост за прошлые периоды.

Тема 2.4. Общество, политика и законодательство. альтернативы proof of work (принцип защиты сетевых систем от злоупотреблением услугами).

Договоренности в мире биткойна. Взаимодействие договоренностей. Программное обеспечение Bitcoin Core. Жесткая вилка в правилах. Корни биткойн. Транзакции объем/день. Общая ценность биткойна. Взаимодействие правительства с биткойном и его попытки регулировать эту валюту. Борьба с отмыванием денег. Регулирование криптовалюты. Общие

требования к алгоритмам PoW (доказательство выполнения работы). Алгоритмы, выполняющие реальную работу. Алгоритмы, защищенные от распределения. Виртуальный майнинг, PoS (материалы, способствующие продвижению бренда или товара в местах продаж).

Раздел 3. Основные стратегии торговли на бирже криптовалют. Вывод электронных средств.

Тема 3.1. Практика использования биткоин в разных областях. экосистемы криптовалют.

Биткойн как журнал только для добавления данных. Практические применения свойств биткоина. Безопасные многопартийные лотереи в биткойне. Биткойн как источник случайности. Рынки прогнозирования и реально существующий поток данных. Разнообразие криптовалют. Взаимодействие электронных бирж. Перекрестные цепи атомарных свопов (финансовая операция в виде обмена разнообразными активами). Плюсы и минусы разнообразия альткоинов. Взаимодействие биткоина и альткоина. Сайдчейн (боковая цепь).

Тема 3.2. Инвестиции в первичное размещение монет (ICO). Технический анализ и продвинутые тактики торговли.

Виды технического анализа. Основные характеристики графического, индикаторного, волнового и свечного анализов.

Тема 3.3. Перспективы развития биткойна.

Технология блокчейн как средство децентрализации. Пути интеграции блокчейна. Краудфандинг (коллективное финансирование основанное на добровольных взносах). Технологии блокчейн, как децентрализованная модель. Сеть долговых обязательств. Преимущества и недостатки децентрализации.

4. Методические рекомендации по организации изучения учебной дисциплины

Изучение дисциплины включает контактную работу обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях в форме занятий различных типов в соответствии со спецификой дисциплины и самостоятельную работу обучающихся в объемах соответственно учебному плану. Контактная работа может проводиться с применением электронного обучения, дистанционных образовательных технологий.

Теоретические занятия

Лекция 1. Тема 1.1. Биткойн и альтернативные криптовалюты.

Криптографические хэш-функции. Хеш-указатели и структуры данных.

Лекция 2. Тема 1.2. Создание электронного кошелька и работа с ним. Сделки с биткоином.

Рассказать о Blockchain info. Механизмы стимулирования, использующиеся в биткоин.

Лекция 3. Тема 1.3. Транзакции, хранение и использование криптовалюты.

Децентрализованная согласованность. Проверка подлинности транзакций майнерами. Скрипты Биткоина. Приложения из скриптов Биткоина. Структура блока Биткоина. Сеть Биткоина. Хранение биткоинов. Горячее и холодное хранилища. Разделение и распространение ключей. Онлайн-кошельки и обменные биржи.

Лекция 4. Тема 2.1 Динамика и аппаратное обеспечение майнинга.

Микширование (смешивание). Алгоритм объединения монет. Tor (система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания) и Шелковый путь.

Лекция 5. Тема 2.2. Исследование криптовалюты для инвестирования.

Определение криптопортфеля и его назначение. Экспертное мнение Джона Маккафи. Проект ICO.

Лекция 6. Тема 2.3. Система инвестирования – критерий при выборе криптовалюты.

Краткосрочное и долгосрочное инвестирование в электронную денежную единицу.

Лекция 7. Тема 2.4. Общество, политика и законодательство. альтернативы proof of work (принцип защиты сетевых систем от злоупотреблением услугами).

Договоренности в мире биткойна. Взаимодействие договоренностей. Программное обеспечение Bitcoin Core.

Лекция 8. Тема 3.1. Практика использования биткоин в разных областях. экосистемы криптовалют.

Биткойн как источник случайности. Рынки прогнозирования и реально существующий поток данных. Разнообразие криптовалют. Взаимодействие электронных бирж.

Лекция 9. Тема 3.2. Инвестиции в первичное размещение монет (ICO). Технический анализ и продвинутые тактики торговли.

Виды технического анализа. Основные характеристики графического, индикаторного, волнового и свечного анализов.

Лекция 10. Тема 3.3. Перспективы развития биткойна.

Технология блокчейн как средство децентрализации. Пути интеграции блокчейна. Краудфандинг (коллективное финансирование основанное на добровольных взносах). Технологии блокчейн, как децентрализованная модель. Сеть долговых обязательств. Преимущества и недостатки децентрализации.

Практические занятия

Тема 1.1. Биткойн и альтернативные криптовалюты.

Практическое применение хеш-функции для генерации электронной денежной единицы.

Тема 1.2. Создание электронного кошелька и работа с ним. Сделки с битконом.

Алгоритм создания электронного кошелька его возможности и надежность. Практическая транзакция из одного электронного кошелька в другой.

Тема 1.3. Транзакции, хранение и использование криптовалюты.

Практическое ведение журнала (реестр) в режиме Append-Only. Присоединение к пиринговой сети Биткоина.

Тема 2.1 Динамика и аппаратное обеспечение майнинга.

Практическая реализация углубленной схемы SHA-256.

Тема 2.2. Исследование криптовалюты для инвестирования.

Формирование криптопортфеля его динамика.

Тема 2.3. Система инвестирования – критерий при выборе криптовалюты

Расчет показателей соотношение риск/прибыль, снижение цены/рост за прошлые периоды.

Тема 2.4. Общество, политика и законодательство. альтернативы proof of work (принцип защиты сетевых систем от злоупотреблением услугами).

Общие требования к алгоритмам PoW (доказательство выполнения работы). Алгоритмы, выполняющие реальную работу. Алгоритмы, защищенные от распределения. Виртуальный майнинг, PoS (материалы, способствующие продвижению бренда или товара в местах продаж).

Тема 3.1. Практика использования биткоин в разных областях. экосистемы криптовалют.
Практические применения свойств биткоина.
Тема 3.3. Перспективы развития биткойна.
Применение технологии блокчейн для работы с криптовалютой.

5. Методические рекомендации для обеспечения самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студентов включает усвоение теоретического материала, подготовку к практическим занятиям, выполнение самостоятельных заданий, творческих заданий, изучение литературных источников, использование Internet-данных, изучение нормативно-правовой базы, подготовку к текущему контролю знаний, к промежуточной аттестации.

Вопросы для самоконтроля

1. Выполнить сравнительный анализ по генерации криптовалюты с помощью двух алгоритмов и программ представленных ниже
2. Выполнить установку и настройку программ для майнинга криптовалюты под Windows
3. Выполнить установку и настройку программ для майнинга криптовалюты под Linux

1. Алгоритм Cryptonight.
2. Алгоритм Cryptonote
3. Алгоритм x11
4. Алгоритм Dagger-Hashimoto
5. Алгоритм Equihash
6. NHegMiner
7. Wolf’s cpu miner,
8. Claymore cpu,
9. Yam cpu,
10. Cminer
11. CGminer
12. Guiminer
13. ethminer,
14. nheqminer.
15. BitcoinCOr
16. MinerGate
17. AwesomeMner

6. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

6.1 Планируемые результаты обучения, обеспечивающие достижение планируемых результатов освоения образовательной программы

В процессе изучения дисциплины у обучающихся должны быть сформированы следующие компетенции:

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

Индикаторы достижения компетенций	Планируемые результаты обучения
ИД-1 (УК-1). Выполняет поиск необходимой информации, её критический анализ и обобщает результаты анализа для решения поставленной задачи.	***знает***
	РО-1 ИД -1 (УК-1) теоретические основы криптографии; методов и способов генерации криптовалют, основы экономических знаний в различных сферах деятельности по учету и оценке различных криптовалют
	умеет
	РО-2 ИД -1 (УК-1) использовать основы экономических знаний для обращения с криптовалютой; позиционировать электронное предприятие на глобальном рынке; применять основные экономические понятия при использовании различных электронных активов, в том числе криптовалют;
ИД-2 (УК-1). Использует системный подход для решения поставленных задач.	***знает***
	РО-1 ИД -2 (УК-1) практики продвижения инновационных программно-информационных продуктов и услуг; современных программных продуктов и средств для работы с крипто валютой
	умеет
	РО-2 ИД -2 (УК-1) использовать лучшие практики продвижения инновационных программно-информационных продуктов и услуг; формировать потребительскую аудиторию и осуществлять взаимодействие с потребителями; **РО-3 ИД -2 (УК-1)** пользоваться навыками применения системного подхода для решения поставленных задач.

6.2 Перечень оценочных материалов

Оценочные материалы представляют собой задания для выполнения студентом, позволяющие ему приобрести теоретические знания, практически умения (навыки) и опыт, а также решать задачи, связанные с будущей профессиональной деятельностью. Включают в себя задания для текущего контроля уровня успеваемости, оценивающие ход освоения учащимися дисциплины, и задания для промежуточной аттестации обучающих, обеспечивающие оценивание промежуточных и окончательных результатов обучения по дисциплине.

Примерные задания для проведения текущего контроля успеваемости

Темы докладов (сообщений)

1. Хэш-функции
2. Блокчейн
3. Деревья Меркля.
4. Свойства деревьев Меркля
5. Отсортированное дерево Меркля
6. структура Меркла-Дамгарда
7. Цифровая подпись
8. Схема цифровой подписи.
9. Свойства цифровой подписи.
10. Схема цифровой подписи ECDSA
11. Публичные ключи
12. Простейшая криптовалюта GoofyCoin
13. Криптовалюта ScroogeCoin
14. Транзакции
15. Децентрализация
16. Распределенный консенсус
17. Протокол распределенного консенсуса
18. Алгоритм консенсуса биткоина
19. Атака двойной траты
20. Награда за блок.
21. Параметрируемая стоимость.
22. Плотность вероятности функции времени до нахождения следующего блока.
23. Стоимость майнинга
24. Премайн
25. Механика биткоина
26. Биткоин-транзакции
27. Транзакция биткоина
28. Сценарный язык биткоина.
29. Исполнение биткоин-скрипта.

Тест

1. У Алисы есть 30 монет, 15 монет она хочет перевести Бобу, а 15 оставить себе. Что она должна сделать?
   а) создать транзакцию с переводом 15 монет Бобу
   б) создать транзакцию с переводом 15 монет Бобу, 15 монет Банку
   в) создать транзакцию с переводом 15 монет Бобу, 15 медиатору
   г) создать транзакцию с переводом 15 монет Бобу и 15 самой себе

2. Каким методом проверяется действительность транзакций в Биткоин?
   а) методом прямого бесконечного поиска
   б) методом обратного бесконечного поиска
   в) методом прямого конечного поиска
   г) методом обратного конечного поиска

3. Из каких частей состоит транзакция?
   а) серия входов и серия выходов
   б) метаданные, серия входов и серия выходов
   в) заголовок и серия выходов
   г) серия выходов и метаданные

4. В скрипте scriptPublicKey используется параметр PubKeyHash. Что это такое?
   а) хеш открытого ключа получателя
   б) подпись транзакции получателем
   в) хеш закрытого ключа получателя
   г) хеш открытого ключа отправителя

5. Какой механизм в схеме с залоговой стоимостью позволяет Джуди, которая выступает в роли судьи, не вступать в спор, пока он не появится?
   а) MULTISIG
   б) P2SH
   в) CHECKSIG
   г) OP_RETURN

6. Какой способ использования скриптов подходит для ситуации, хочет оплатить Бобу каждую минуту услуги, но при этом не хочет создавать новые транзакции ежеминутно??
   а) микротранзакции
   б) оплата по хэшу
   в) условные транзакции
   г) зеленые адреса

7. Если две конфликтные сделки A -> B и A -> C начнут почти одновременно продвигаться из разных узлов, то что определит итоговое помещение одной из этих сделок в блокчейн?
   а) будет выбрана сделка, которая распространилась на наибольшее число узлов

б) выбор будет сделан майнером, который добавит одну из сделок в блок

в) каждый узел имеет свое представление о блокчейне, храня в себе информацию о тех сделках, о которых он узнал

г) будет выбрана сделка, которая начала распространяться раньше

8. Блоки содержат дерево сделок вместо простого листа потому, что:

а) таким образом становится проще добавлять или удалять новые транзакции, когда блок находится в собранном состоянии

б) это позволяет эффективно доказать, что сделка включена в блок

в) это уменьшает размер блоков

г) экономит ресурсы сети

9. Почему пропускная способность Биткоина ограничена?

а) потому что майнеры не могут наращивать свои мощности бесконечно

б) потому что размер одного блока был изначально строго закодирован

в) потому что существует конечное число биткоинов

г) потому что в транзакции указан параметр lock_time

10. Чтобы транзакция была успешно завершена, необходимо…

а) серия чтобы скрипт scriptSig вернул значение «true»

б) чтобы у получателя была пара открытый и закрытый ключи

в) чтобы единый скрипт, состоящий из scriptSig и scriptPublicKey, вернул значение «true»

г) чтобы скрипт scriptPublicKey вернул значение «true»

11. Элис платит за услугу Бобу, используя микро транзакции. Если она внезапно отключится, не предупредив Боба, и перестанет пересылать оплату, то что может сделать Боб в такой ситуации?

а) Боб может извлечь то максимальное значение, указанное Элис в MULTISIG

б) Боб получит сумму по микро транзакции, которую Элис подписала перед отключением

в) Боб может отказаться подписывать возвратную транзакцию

г) Бобу ничего не сможет сделать, чтобы получить свои деньги

12. Боб получил 5 монет от Алисы и 10 от Чака. Как он может объединить две разные транзакции в одну?

а) это невозможно

б) создать транзакцию с одним входом (5 и 10) и двумя выходами (5 и 10)

в) создать транзакцию с двумя входами (5 и 10) и одним выходом (15)

г) с помощью третьей стороны

13. Выделите верное утверждение.

а) адрес ввода указывается в виде скрипта, адрес вывода – в виде открытого ключа

б) адрес ввода и вывода указываются в виде открытых ключей

в) адрес ввода и вывода указываются в виде скриптов

г) адрес ввода указывается в виде открытого ключа, адрес вывода – в виде скрипта

14. Что из перечисленного требует для себя «твердой вилки» (выберите все правильные ответы):
    а) понижение максимально доступного размера блоков
    б) добавление новой инструкции OP_SHA3
    в) повышение максимально доступного размера блока
    г) отключение инструкции OP_SHA1

15. Выберите верное утверждение.
    а) новые узлы подключаются в любое время
    б) новые узлы подключаются, если у них есть разрешение майнера
    в) новые узлы подключаются по расписанию заголовок и серия выходов
    г) количество узлов не меняется с момента создания сети

Творческие задания.

Использовать лучших практик продвижения инновационных программно-информационных продуктов и услуг

Провести сравнительный анализ двух стратегий торговли на бирже бинарных опционов. Провести статистический анализ для 20 сделок на разных временных промежутках. Стратегии представлены после таблицы №1. При тестировании желательно использовать торгового брокера «Binomo».

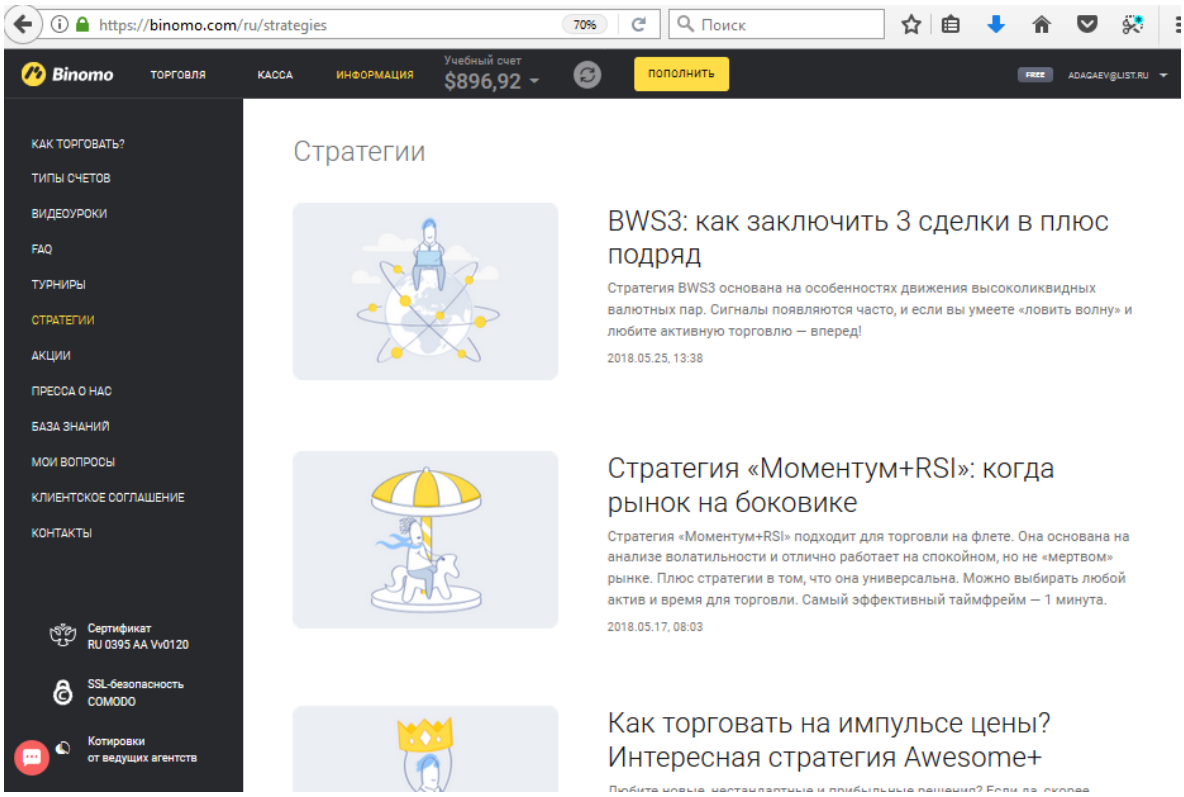

Рис.2 Стратегии на сайте Binomo

Задания по вариантам

Таблица №1

Номер варианта	Номера стратегий
1.	1-9
2.	2-8
3.	3-7
4.	4-10
5.	5-11
6.	6-12
7.	7-13
8.	12-28
9.	13-29
10.	14-30
11.	15-31
12.	16-32
13.	17-33
14.	18-34
15.	19-35
16.	20-36
17.	21-37
18.	22-38
19.	23-39
20.	24-40
21.	25-41
22.	26-42
23.	27-43
24.	28-44
25.	29-45
26.	46-61
27.	47-62
28.	48-63
29.	49-64
30.	50-65
31.	51-65
32.	52-66
33.	53-67
34.	54-68
35.	55-69
36.	56-70
37.	57-58

Перечень торговых стратегий

1. Моментум+RSI»
2. Awesome+

3. ATR+ФИБО: торговля на пробое волатильности
4. ADX+RSI: успешная торговля в любое время на любом активе
5. Облако Ichimoku
6. SEER: стратегия на любой случай
7. Фракталы CCI
8. Стохастик X2
9. Индикатор Моментум DC
10. Parabolic SAR
11. ADX + Stoch
12. «Зигзаг по Боллинджеру»
13. Новые грани MACD (9:20)
14. Минута разворота
15. «Все включено»: стратегия для флета
16. «Возврат»: стратегия для торговли с 23:00 до 03:00 Мск
17. Beep Фибо
18. «60 секунд»
19. Gould
20. Guppy: стратегия с 13-ю скользящими средними
21. «Звезды»: стратегия со свечными паттернами
22. «Облака»
23. Быстрый Джон
24. Три свечи+Следопыт
25. Дыхание рынка
26. Нос Пиноккио
27. Багги
28. Наблюдатель на свечах
29. Схождение/расхождение рынка с RSI
30. Пробой Фибоначчи
31. YenBB: стратегия для торговли на японской иене
32. Две волны
33. Три свечи
34. Гартли
35. Пробой «Вил Эндрюса»
36. 20+RSI
37. Drifter
38. Фигура «Флаг»
39. Двойной MACD
40. «Пинг-понг на MACD»
41. «Галстук-бабочка»
42. «Метод Пуриа»
43. «Скользящие каналы Баришпольца»
44. «Разворот на фрактале»
45. Прибыль через минуту: скальпинг на индикаторе MACD
46. «Пробой Боллинджера»
47. «Усреднение»
48. «Дыхание рынка» (на скользящих средних)

49. Торговля по уровням Фибоначчи
50. «Три экрана Элдера»
51. Торговля на дивергенции MACD
52. Racer
53. Wild River
54. HELIX
55. «Вход на откате»
56. Торговля в коридоре цен
57. Торговля на пробой коридора цен
58. «Отскок от линии тренда»
59. «Свечное поглощение: разворот»
60. «Свечное поглощение — продолжение движения»
61. «Скользящие средние с фильтром MACD»
62. Индикатор RSI и стратегия «Разворот на экстремумах»
63. «Волны Боллинджера»
64. «Аллигатор»
65. «Ночной канал»
66. RSI и CCI
67. Горизонт
68. Moving Average, Exponentional, Stochastic.
69. Стратегия на Parabolic SAR
70. Стратегия основанная на ATR

Практические задания

1. Построение хэш- функций

Пусть значения ключа являются неотрицательными целыми числами (так всегда можно интерпретировать представляющую ключ K битовую строку).

Построить ХЭШ-функции и открытые таблицы одним из представленных методов

1.1 Модульное хэширование (метод деления)

В методе деления хеш-функция задаётся как вычет ключа K по модулю некоторого числа m (то есть как остаток от деления нацело K на m):

$$h(K) = K \bmod m.$$

В этом случае хеш-коды ключей образуют множество $\mathrm{H} = \{0,1,\ldots,m-1\}$, и их количество $\left|\mathrm{H}\right| = m$.

Для того чтобы в формировании $h(K)$ участвовали все разряды двоичного представления K, рекомендуется выбирать в качестве модуля m простое число, далёкое от степени двойки.

Максимально возможное число коллизий $l_{\max}$ на единицу больше целой части дроби $|K|/m$:

$$l_{\max} = [|K|/m] + 1.$$

Например, если $K = \{1, 2, ..., 19\}$, то

$$|K| = 19,\ \ m = 3,\ \ [|K|/3] + 1 = 6 + 1 = 7,$$

и семь чисел $1, 4, 7, 10, 13, 16, 19$ имеют одинаковый остаток 1 по модулю 3.

1.2 Закрытое хеширование

При закрытом (внутреннем) хешировании в хеш-таблице хранятся непосредственно сами элементы, а не заголовки списков элементов. Поэтому в каждой записи (сегменте) может храниться только один элемент. При закрытом хешировании применяется методика повторного хеширования. Если осуществляется попытка поместить элемент k в сегмент с номером h(k), который уже занят другим элементом (такая ситуация называется коллизией), то в соответствии с методикой повторного хеширования выбирается последовательность других номеров сегментов h 1 (k), h 2 (k), ..., куда можно поместить элемент k. Каждое из этих местоположений последовательно проверяется, пока не будет найдено свободное. Если свободных сегментов нет, то, следовательно, таблица заполнена, и элемент k добавить нельзя.

Алгоритм включения

```
Insert (T, k)
1. i←0
2. repeat
3. j←h(k,i)
4. if T[j]=nil then
5. T[j]←k, return j
6. else i←i+1
7. until i=m
8. printf “Хеш – таблица переполнена”
```

Алгоритм поиска

```
Search (T, k)
1. i←0
2. repeat
3. j←h(k,i)
4. if T[j]=k then return j
5. i←i+1
6. until ((T[j]=nil or (i=m))
return nil
```

Существует несколько методов повторного хеширования:

1. Линейное опробование сводится к последовательному перебору сегментов таблицы с некоторым фиксированным шагом:

h(k, i) = (h / (k, i)) mod m

i – номер пробы

Минус: метод приводит к образованию кластеров (когда несколько ячеек подряд заняты). Кластер приводит к тому, что увеличивается время доступа к данным.

2. Квадратичное опробование отличается от линейного тем, что шаг перебора сегментов нелинейно зависит от номера попытки найти свободный сегмент:

h(k, i) = (h / (k) + i 2) mod m

Благодаря нелинейности такой адресации уменьшается число проб при большом числе ключей-синонимов.

Однако даже относительно небольшое число проб может быстро привести к выходу за адресное пространство небольшой таблицы вследствие квадратичной зависимости адреса от номера попытки.

3. Двойное хеширование основано на нелинейной адресации, достигаемой за счет суммирования

значений основной и дополнительной хеш-функций:

h(k, i) = (h 1 (k,i) + h 2 (k, i)) mod m

«+» У каждого ключа свой шаг проб.

1.3 Метод умножения

Пусть желаемое количество различных хеш-кодов равно m. *Выберем некоторое число* $a \in (0,1)$. *В методе умножения хеш-функция задаётся формулой:*

$$h(K) = [m \cdot \{Ka\}],$$

то есть $h(K)$ — целая часть произведения m на дробную часть числа Ka. Например, если $K = 1208,\ a = 0.017,\ m = 100$, то $Ka = 20.536$, $\{Ka\} = 0.536$, $m \cdot 0.536 = 53.6$, $h(K) = [53.6] = 53$.

Возможна следующая модификация метода умножения. Пусть битовая строка для представления ключа K имеет l разрядов. В качестве m можно выбрать степень двойки: $m = 2^j$, где $j < l$. Выберем некоторое $s \in (0, 2^l)$ и положим $a = s / 2^l$. Тогда вычисление Ka можно провести, минуя деление:

$$Ka = K \cdot (s / 2^l) = (Ks) / 2^l.$$

Произведение целых чисел Ks занимает $2l$ битов, и переход от Ks к $[Ks / 2^l]$ приводит к l младшим разрядам произведения Ks. Теперь в качестве кода $h(K)$ можно взять j старших из этих l разрядов.

1.4 Динамическое хеширование

Основной принцип динамического хеширования заключается в обработке числа, выработанного хеш-функцией в виде последовательности битов, и распределении записей по сегментам на основе так называемой прогрессирующей оцифровки этой последовательности. Динамическая хеш-функция вырабатывает значения в широком

диапазоне, а именно ***b***-битовые двоичные целые числа, где ***b*** обычно равно 32. Такой способ организации показан на рисунке 1.

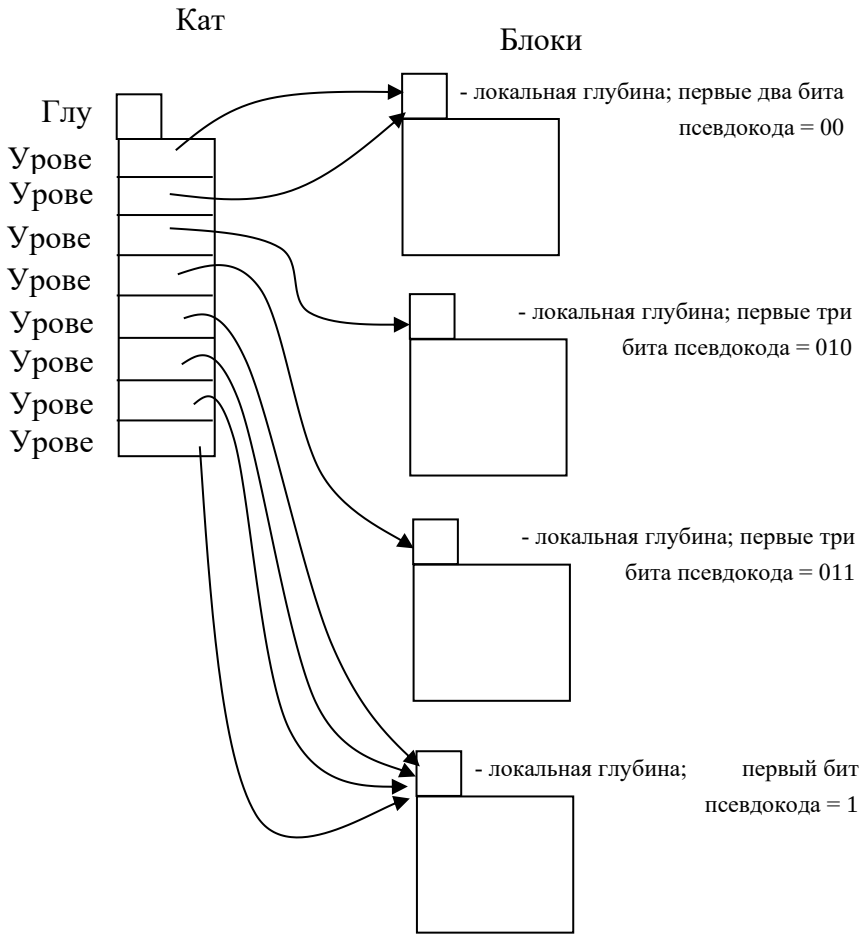

Рис.1 – Динамическое хеширование

1.5 Универсальное хэширование

Универсальное хеширование основано на принципе случайного выбора хеш-функции $\mathrm{K} \xrightarrow{h_i} \mathrm{H}$ из некоторого заранее сформированного множества $\Phi = \{h_1, h_2, ..., h_r\}$ при каждом запуске алгоритма хеширования. Благодаря этому хеширование не будет работает постоянно плохо (то есть не будет давать неприемлемо большое число коллизий) даже для таких совокупностей ключей, на которых плохо работает некоторая фиксированная хеш-функция.

Множество хеш-функций Φ называется *универсальным*, если для каждой пары ключей $K, K' \in \mathrm{K}$ при случайном выборе h вероятность коллизии не превосходит $1/m$:

$P(h(K) = h(K')) \le 1/m$.

Последнее означает, что доля в H тех функций, для которых $h(K) = h(K')$, не превосходит $1/m$.

Универсальное множество Φ можно построить, например, следующим образом (ключ K, напомним, интерпретируется как натуральное число, $m = |\mathrm{H}|$). Пусть $\mathbf{Z}_p = \{0,1,...,p-1\}$ — полная система вычетов по *простому* модулю $p > m$, $\mathbf{Z}_p^* = \{1,...,p-1\}$ — система ненулевых вычетов. Если $a \in \mathbf{Z}_p^*,\ b \in \mathbf{Z}_p$, то определяем хеш-функцию $h_{a,b} \in \Phi$ формулой

$h_{a,b}(K) = r \bmod m$,

где $r = (aK + b) \bmod p \in \mathbf{Z}_p$ — остаток целочисленного деления $aK + b$ на p. Количество таких функций $|\Phi| = (p-1)p$.

1.6 Минимальное идеальное хеширование

Идеальной хеш-функцией называется такая функция, которая отображает каждый ключ из набора S в множество целых чисел без коллизий. В математических терминах это инъективное отображение.

Описание

Функция $h(k): U \to [m]$ *называется идеальной хеш-функцией для* $S \subseteq U$*, если она инъективна на* S*;*

1. Функция $h(k): U \to [m]$ называется минимальной идеальной хеш-функцией для $S \subseteq U$, если она является ИХФ и $m = n = |S|$;
2. Для целого $k \geq 1$, функция $h(k): U \to [m]$ называется k-идеальной хеш-функцией (k-PHF) для $S \subseteq U$ если для каждого $j \in [m]$ имеем $|\{x \in S | h(x) = j\}| \leq k$.

Идеальное хеширование применяется в тех случаях, когда мы хотим присвоить уникальный идентификатор ключу, без сохранения какой-либо информации о ключе. Одним из наиболее очевидных примеров использования идеального (или скорее k-идеального) хеширования является ситуация, когда мы располагаем небольшой быстрой памятью, где размещаем значения хешей, связанных с данными хранящимися в большой, но медленной памяти. Причем размер блока можно выбрать таким, что необходимые нам данные, хранящиеся в медленной памяти, будут получены за один запрос. Подобный подход используется, например, в аппаратных маршрутизаторах. Также идеальное хеширование используется для ускорения работы алгоритмов на графах, в тех случаях, когда представление графа не умещается в основной памяти.

1.7 Расширяемое хеширование (extendible hashing)

Расширяемое хеширование сочетает свойства методов хеширования, алгоритмов на основе многопутевых trie-деревьев и методов последовательного доступа. Подобно методам хеширования, описанным в "Хеширование" , расширяемое хеширование представляет собой рандомизированный алгоритм — поэтому сначала необходимо определить хеш-функцию, которая преобразует ключи в целые числа (см. раздел 14.1 "Хеширование"). Для простоты в этом разделе мы будем просто считать, что ключи

являются случайными битовыми строками фиксированной длины. Подобно алгоритмам с использованием многопутевых trie-деревьев из "Поразрядный поиск" , расширяемое хеширование начинает поиск, используя ведущие разряды ключей в качестве индексных указателей в таблице, размер которой равен степени 2. Подобно алгоритмам на основе B-деревьев, при использовании расширяемого хеширования элементы хранятся в страницах, которые при заполнении разбиваются на две части. Подобно методам индексно-последовательного доступа, расширяемое хеширование поддерживает каталог, указывающий, где можно найти страницу, в которой находятся соответствующие искомому ключу элементы. Сочетая эти знакомые свойства в одном алгоритме, расширяемое хеширование как нельзя более подходит для завершения знакомства с алгоритмами поиска.

Предположим, что количество доступных страниц диска является степенью 2 — скажем, 2^d. Тогда можно поддерживать каталог 2^d различных ссылок на страницы, использовать d разрядов ключей для индексного доступа к этому каталогу и хранить в одной и той же странице все ключи, первые к разрядов которых совпадают (см. рис.2). Как и в случае B-деревьев, элементы на страницах хранятся упорядоченными, и, найдя страницу, которая соответствует элементу с заданным искомым ключом, мы выполняем в ней последовательный поиск.

На рис.2 приведены две базовых концепции, лежащие в основе расширяемого хеширования. Во-первых, совсем не обязательно поддерживать 2^d страниц. То есть можно иметь несколько записей каталога со ссылками на одну и ту же страницу, объединив на одной странице ключи с различными значениями, первые d разрядов которых совпадают.

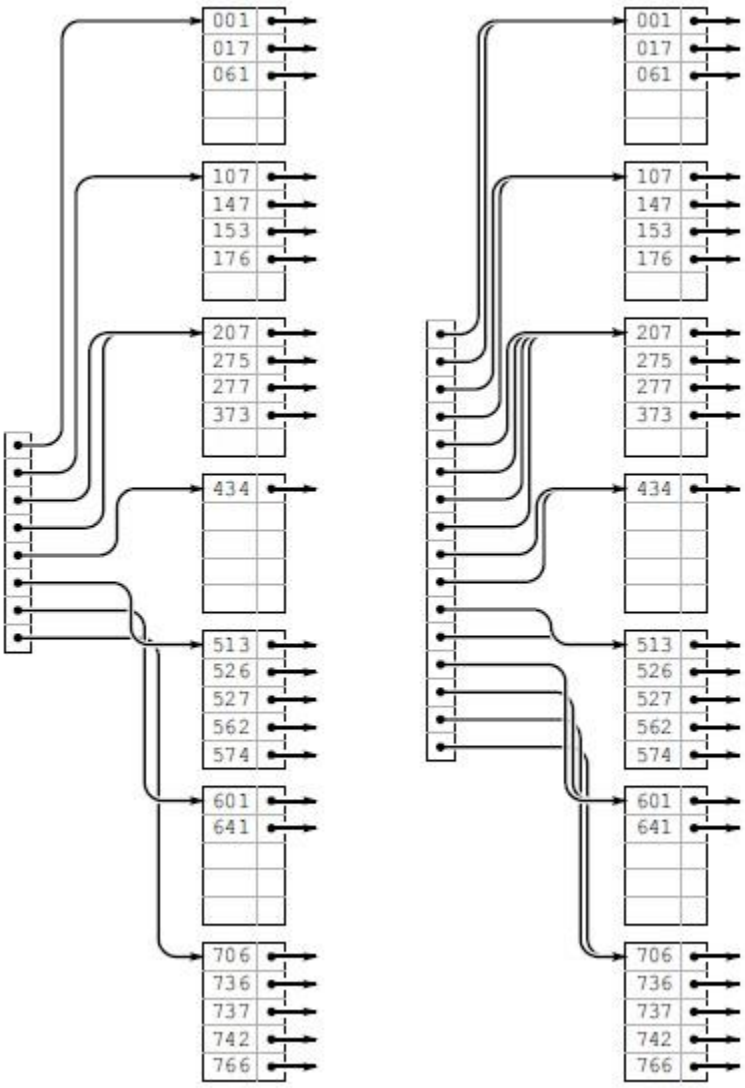

Рис.2 Индексы страниц каталога

Каталог, состоящий из восьми записей, позволяет содержать до 40 ключей, храня все записи с первыми 3 совпадающими разрядами на одной странице, обратиться к которой можно через ссылку, хранящуюся в каталоге (слева). Запись 0 каталога содержит ссылку на страницу, которая содержит все ключи, начинающиеся с 000; запись 1 таблицы содержит ссылку на страницу, которая содержит все ключи, начинающиеся с 001; запись 2 таблицы содержит ссылку на страницу, которая содержит все ключи, начинающиеся с 010, и т.д. Если некоторые страницы заполнены не полностью, количество требуемых страниц можно уменьшить, используя несколько ссылок на одну и ту же страницу. В данном примере (слева) ключ 3 73 находится на той же странице, что и ключи, начинающиеся с 2; эта страница определена как содержащая элементы с ключами, первые два разряда которых равны 01.

Если удвоить размер каталога и скопировать каждую ссылку, то получим структуру, которую можно индексировать первыми 4 разрядами искомого ключа (справа). Например, последняя страница по-прежнему определяется как содержащая элементы с ключами, первые три разряда которых равны 111, и она будет доступна через каталог для искомых ключей с первыми 4 разрядами 1110 или 1111. Этот больший каталог допускает увеличение таблицы.

Это не помешает быстро выполнять поиск в структуре и в то же время позволяет находить страницу с искомым ключом, используя ведущие разряды ключа для индексного доступа к каталогу. Во-вторых, для увеличения емкости таблицы можно удваивать размер каталога.

В частности, структура данных, которая применяется для расширяемого хеширования, значительно проще используемой в B-деревьях. Она состоит из страниц, содержащих до M элементов, и каталога с 2^d ссылками на страницы (см. программу 16.5). Ссылка в ячейке каталога x указывает на страницу, содержащую все элементы с ведущими d разрядами, равными x. Значение d выбирается достаточно большим, чтобы в каждой странице гарантированно хранилось менее M элементов. Реализация операции найти проста: мы используем ведущие d разрядов ключа для индексного доступа к каталогу, что обеспечивает доступ к странице, которая содержит все элементы с соответствующими ключами, а затем выполняем последовательный поиск такого элемента на данной странице (см. программу 16.6).

Для поддержки операции вставить структура данных должна быть несколько более сложной, однако одно из ее свойств заключается в том, что этот алгоритм поиска успешно работает без каких-либо модификаций. Но сначала необходимо ответить на следующие вопросы:

- Что делать, когда количество элементов на странице превысит ее емкость?
- Какой размер каталога следует использовать?

2. Построение хэш-таблиц

Построить хэш-таблицу с применением одного из алгоритмов, оценить количество коллизий для открытой таблицы в миллион строк.

1. CRC32
2. MD4
3. MD5
4. SHA1
5. SHA256
6. SHA512

3. Тестирование хеш-таблиц

При выполнении лабораторных для оценки и сравнения работы хеш-таблиц необходимо использовать тестовые данные, выданные преподавателем. Тестовые данные содержат тексты на английском языке из различных областей. Целью лабораторной работы является анализ частоты встречаемости слов во входном тексте с применением хеш-таблицы, соответствующей заданию.

Входной текст разбивается на слова, очищается от знаков препинания и помещается в хеш- таблицу. Каждый элемент хеш-таблицы - это слово и поле-счетчик, содержащее количество раз, которое данное слово встретилось в тексте. При вставке нового элемента в таблицу, если данный элемент уже присутствует в ней, необходимо увеличить соответствующий счетчик. В противном случае создается новый элемент. Программа должна выдавать 10 слов, которые встречаются чаще всего во входном тексте.

Также каждый вариант содержит дополнительное задание.

Операции вставки, поиска и удаления элементов должны быть реализованы в виде отдельных функций.

Для оценки времени работы некоторой функции func() использовать функцию gettimeofday().

Для успешной компиляции необходимо подключить файл time.h (#include <sys/time.h>). Данный файл содержит определение структуры timeval:

```
struct timeval {
time_t tv_sec; /* seconds */
suseconds_t tv_usec; /* microseconds */
};
```

Вычисление времени работы func() определяется по аналогии со следующим листингом:

```
#include <stdio.h>
#include <sys/time.h>
void func()
{
sleep (1);
}
int main()
{
struct timeval tv1, tv2; float start, end, func_time;
gettimeofday(&tv1,NULL); func();
gettimeofday(&tv2,NULL); tv2.tv_sec -= tv1.tv_sec; tv1.tv_sec = 0;
start = tv1.tv_sec + (float)tv1.tv_usec*1E-6;
end = tv2.tv_sec + (float)tv2.tv_usec*1E-6;
func_time = end - start;
printf("func_time = %f\n",func_time);
}
```

Рис 1. Определение времени работы функции func()

Примерные задания для проведения промежуточной аттестации по дисциплине

Список экзаменационных вопросов

РО-1 ИД -1 (УК-1) теоретические основы криптографии; методов и способов генерации криптовалют, основы экономических знаний в различных сферах деятельности по учету и оценке различных криптовалют

1. Эскроу-транзакции.
2. Зелёный адрес.
3. Сжигание.
4. Эффективные микроплатежи.
5. Время блокировки.
6. Биткоин-блоки
7. Биткоин-сеть

РО-1 ИД -2 (УК-1) практики продвижения инновационных программно-информационных продуктов и услуг; современных программных продуктов и средств для работы с крипто валютой

8. Время распространения блока.
9. Размеры сети.
10. Размер блокчейна.
11. Лёгкие узлы.
12. Ограничения биткоин-протокола
13. Хардфорк, софтфорк
14. ранение битокина
15. Кошельки для криптовалюты
16. Горячее и холодное хранение
17. Иерархические кошельки

РО-2 ИД -2 (УК-1) использовать лучшие практики продвижения инновационных программно-информационных продуктов и услуг; формировать потребительскую аудиторию и осуществлять взаимодействие с потребителями;

18. Схема иерархического ключа.
19. Методы хранения информации в оффлайне
20. Фракционирование
21. Математика фракционирования.
22. Пороговая криптография
23. Мультисигнатурность
24. Онлайн-кошельки
25. Биткоин-биржи
26. Три вида рисков.

РО-3 ИД -2 (УК-1) пользоваться навыками применения системного подхода для решения поставленных задач

27. Доказательство резерва.
28. Доказательство обязательств
29. Доказательство включение на дереве Меркла
30. Платёжные сервисы

6.3. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Для оценивания результатов промежуточной аттестации применяется шкала оценивания, включающая следующие оценки: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Экзамен. Критерии выставления оценок

На экзамен выносятся вопросы, охватывающие все содержание учебной дисциплины.

Знания обучающихся оцениваются путем выставления по результатам ответа обучающегося итоговой оценки «отлично», либо «хорошо», либо «удовлетворительно», либо «неудовлетворительно».

Оценка «отлично» при приеме экзамена выставляется в случае:

- полного, правильного и уверенного изложения обучающимся учебного материала по каждому из вопросов билета;
- уверенного владения обучающимся понятийно-категориальным аппаратом учебной дисциплины;
- логически последовательного, взаимосвязанного и правильно структурированного изложения обучающимся учебного материала, умения устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;
- приведения обучающимся надлежащей аргументации, наличия у обучающегося логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам билета;
- лаконичного и правильного ответа обучающегося на дополнительные вопросы преподавателя.

Оценка «хорошо» при приеме экзамена выставляется в случае:

- недостаточной полноты изложения обучающимся учебного материала по отдельным (одному или двум) вопросам билета при условии полного, правильного и уверенного изложения учебного материала по, как минимум, одному вопросу билета;
- допущения обучающимся незначительных ошибок и неточностей при изложении учебного материала по отдельным (одному или двум) вопросам билета;
- допущения обучающимся незначительных ошибок и неточностей при использовании в ходе ответа отдельных понятий и категорий дисциплины;
- нарушения обучающимся логической последовательности, взаимосвязи и структуры изложения учебного материала по отдельным вопросам билета, недостаточного умения обучающегося устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;
- приведения обучающимся слабой аргументации, наличия у обучающегося недостаточно логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам билета;
- допущения обучающимся незначительных ошибок и неточностей при ответе на дополнительные вопросы преподавателя.

Любой из указанных недостатков или их определенная совокупность могут служить основанием для выставления обучающемуся оценки «хорошо».

Оценка «удовлетворительно» при приеме экзамена выставляется в случае:

- невозможности изложения обучающимся учебного материала по любому из вопросов билета при условии полного, правильного и уверенного изложения учебного материала по как минимум одному из вопросов билета;
- допущения обучающимся существенных ошибок при изложении учебного материала по отдельным (одному или двум) вопросам билета;
- допущении обучающимся ошибок при использовании в ходе ответа основных понятий и категорий учебной дисциплины;

• существенного нарушения обучающимся или отсутствия у обучающегося логической последовательности, взаимосвязи и структуры изложения учебного материала, неумения обучающегося устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;

• отсутствия у обучающегося аргументации, логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам билета;

• невозможности обучающегося дать ответы на дополнительные вопросы преподавателя.

Любой из указанных недостатков или их определенная совокупность могут служить основанием для выставления обучающемуся оценки «удовлетворительно».

Оценка «неудовлетворительно» при приеме экзамена выставляется в случае:

• отказа обучающегося от ответа по билету с указанием, либо без указания причин;

• невозможности изложения обучающимся учебного материала по двум или всем вопросам билета;

• допущения обучающимся существенных ошибок при изложении учебного материала по двум или всем вопросам билета;

• скрытное или явное использование обучающимся при подготовке к ответу нормативных источников, основной и дополнительной литературы, конспектов лекций и иного вспомогательного материала, кроме случаев специального указания или разрешения преподавателя;

• невладения обучающимся понятиями и категориями данной дисциплины;

• невозможность обучающегося дать ответы на дополнительные вопросы преподавателя;

Любой из указанных недостатков или их совокупность могут служить основанием для выставления обучающемуся оценки «неудовлетворительно».

Обучающийся имеет право отказаться от ответа по выбранному билету с указанием, либо без указания причин и взять другой билет. При этом с учетом приведенных выше критериев оценка обучающемуся должна быть выставлена на один балл ниже заслуживаемой им.

Дополнительные вопросы могут быть заданы обучающемуся в случае:

• необходимости конкретизации и изложенной обучающимся информации по вопросам билета с целью проверки глубины знаний отвечающего по связанным между собой темам и проблемам;

• необходимости проверки знаний обучающегося по основным темам и проблемам курса при недостаточной полноте его ответа по вопросам билета.

При проведении промежуточной аттестации в форме тестирования с использованием шкалы, включающей оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», оценивание результата проводится следующим образом:

«**Отлично**» - получают обучающиеся в том случае, если верные ответы составляют от 80% до 100% от общего количества

«**Хорошо**» - получают обучающиеся в том случае, если верные ответы составляют от 71 до 79% от общего количества;

«**Удовлетворительно**» - получают обучающиеся в том случае, если верные ответы составляют 50 –70 % правильных ответов;

«**Неудовлетворительно**» - работа, содержащая менее 50% правильных ответов.

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

Основная литература

1. Максуров, А. А. Криптовалюты и правовое регулирование их обращения : монография / А. А. Максуров. — 2-е изд. — Москва : Дашков и К, 2019. — 356 c. — ISBN 978-5-394-03298-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/85384.html

2. Максуров, А.А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование / А.А. Максуров. – Москва : Дашков и К°, 2020. – 198 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=600313

Дополнительная литература

1. Перспективы криптовалют в современных экономиках / П.В. Трунин, М.Г. Гирич, И.С. Ермохин и др. ; Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации. – Москва : Дело, 2020. – 72 с. : схем., табл., ил. – (Научные доклады: экономика). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612621

2. Тихонова, М.С. Исследование и моделирование влияния факторов кризиса на устойчивость криптовалюты в современной финансовой системе / М.С. Тихонова ; Пермский государственный национальный исследовательский университет. – Пермь : б.и., 2020. – 80 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=597055

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", справочных систем и профессиональных баз данных, необходимых для освоения дисциплины

1. http://biblioclub.ru/ – электронная библиотечная система «Университетская библиотека Онлайн»
2. http://www.iprbookshop.ru/ – электронная библиотечная система IPR BOOKS
3. Справочная правовая система Консультант Бизнес: Версия Проф

Профессиональные базы данных в составе СПС Консультант:

- Законодательство Санкт-Петербурга и Ленинградской области
- Международное право

4. "Консультант Плюс" - законодательство РФ: кодексы, законы, указы, постановления Правительства Российской Федерации, нормативные акты (consultant.ru)

9. Лицензионное программное обеспечение

- Notepad++ 7.5.8
- Python 3.5.6
- Scala 2.12.6
- Kotlin 1.2.71
- MS Windows 7 Профессиональная
- MS Windows 10 Pro
- Moodle 3.8.2.

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

В зависимости от вида проводимых учебных занятий и форм осуществления образовательной деятельности по соответствующей образовательной программе используется следующее материально-техническое обеспечение дисциплины:

- учебные аудитории для проведения занятий лекционного типа (укомплектованные специализированной мебелью и оборудованные техническими средствами обучения, служащими для представления учебной информации большой аудитории, а также имеющие наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации, соответствующие рабочим программам дисциплин);
- учебные аудитории для проведения занятий семинарского типа (с типовым оборудованием, обеспечивающим применение современных информационных технологий, и наглядными пособиями);
- специальные помещения для проведения занятий по дисциплине (в т.ч. лаборатории, оснащенные лабораторным оборудованием, в зависимости от степени сложности), а именно: _____;
- компьютерные классы с демонстрационно-обучающими и обучающе-контролирующими возможностями, доступом к базам данных и Интернет;
- кабинет для занятий по иностранному языку (оснащенный лингафонным оборудованием);
- учебные аудитории для групповых и индивидуальных консультаций;
- учебные аудитории для текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы обучающихся (оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации);
- библиотека (имеющая читальные залы и рабочие места для обучающихся, оснащенные компьютерами с доступом к базам данных и Интернет).

Для инвалидов и лиц с ограниченными возможностями здоровья форма проведения занятий по дисциплине устанавливается образовательной организацией с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья. При определении формы проведения занятий с обучающимся-инвалидом образовательная организация должна учитывать рекомендации, данные по результатам медико-социальной экспертизы, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда. При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности. При необходимости обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.