МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности

(наименование ф-та полностью)

М.О. Таныгин

(подпись, инициалы, фамилия)

« *29* » *августа* 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Технологии распределенных реестров

(наименование учебной дисциплины)

10.04.01 Информационная безопасность, направленность (профиль) «Защищённые информационные системы»

(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Тема №1 «Понятия и определение технологии распределенных реестров»

1. Дайте определение понятий блокчейна и распределенного реестра.
2. Опишите историю развития технологии блокчейн и распределенных реестров.
3. Понятие и особенности развития цифровой экономики.
4. Опишите классификацию распределенных реестров.
5. Правовое регулирование цифровой экономики.
6. Какая структура и жизненный цикл у транзакций.
7. Как устроены блоки транзакций.
8. Опишите механизм формирования цепочки блоков.

Тема №2 «Структура связи в распределенных системах»

1. Опишите протоколы сетевого взаимодействия в распределенных реестрах и блокчейн.
2. Определите понятие одноранговых сетей и опишите принципы их работы.
3. Определите понятие распределенных хеш-таблиц и опишите принципы их работы.
4. Перечислите известные вам алгоритмы консенсуса и опишите принципы их работы.
5. Опишите проблему византийских генералов и ее связь с технологией блокчейн.

Тема №3 «Современные ОС»

1. Опишите назначение, архитектуру и принципы работы реестра Hyperledger Fabric.
2. Перечислите известные вам промышленные распределенные реестры.
3. Перечислите подходы к осуществлению вычислений в распределенных реестрах.
4. Определите понятие смарт-контракта и опишите принципы их работы.
5. Опишите проблемы масштабируемости распределенных реестров и существующие решения.
6. Опишите существующие подходы и нерешенные проблемы в области приватности данных в распределенных реестрах и технологии блокчейн.

Тема №4 «Распределенные файловые системы»

1. Распределенные файловые системы. Требования и особенности реализации файловой модели в РС.
2. Модели файлового сервиса и сервиса каталогов в РС.
3. Инструменты для интеграции LegalTech-решений в сторонние IT-системы.
4. Методы повышения производительности распределенных файловых систем. Задачи и особенности реализации кэширования.
5. Процессы и потоки выполнения в РС. Необходимость и способы организации синхронизации данных между приложениями для операционных систем РС.
6. Методы организации защиты в РС
7. Задачи и способы репликации файлов в распределенных файловых системах.

Тема №5 «Безопасность блокчейн»

1. Определение порядка реализации и защиты прав владельцев криптовалют.
2. Анализ практики российских судов, иностранного законодательства и позиций исследователей криптовалюты в целях ее правового регулирования на территории Российской Федерации.
3. Криптовалюты как объекты прав.
4. Правовое регулирование использования технологий NLP.
5. Приобретение права собственности на NFT.
6. Понятие, правовая природа и проблемы применения смарт-контрактов в гражданском обороте.
7. Правовое регулирование электронных сделок в современном праве.
8. Сферы применения технологии блокчейн и особенности их правового

регулирования.

Критерии оценки:

3-4 балла выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1-2 балла выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 ВОПРОСЫ И ЗАДАНИЯ В ТЕСТОВОЙ ФОРМЕ

Тема 5

1 С помощью использования блокчейн-технологии в юриспруденции возможно:

1. Сократить расходы на бумажный документооборот;
2. Обеспечить необходимый уровень прозрачности сделок;
3. Оба варианта верны.

2 Среди признаков смарт-контракта обычно выделяют:

1. Данный договор существует исключительно в электронной среде и предполагает обязательное использование электронной подписи, основанной на технологии асимметричного шифрования.
2. Направленность на распоряжение цифровым активом.
3. Оба варианта верны.

3 Под информационной системой согласно ст. 2 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» под информационной системой понимается:

1. Совокупность технических и программных средств, организационных методик и персонала, предназначенная для сбора, хранения и передачи данных.
2. Система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.).
3. Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

4 К странам, которые положительно относятся к регулированию криптовалют, относятся:

1. Бразилия, Великобритания, Иордания, Италия, Кипр.
2. Австралия, Аргентина, Германия, США, Швейцария, Дания.
3. Бангладеш, Боливия, Румыния, Эквадор, Тайвань.

5 В российской доктрине и правоприменительной практике криптовалюта в системе объектов гражданских прав обычно относится к:

1. Иному имуществу.
2. Объектам интеллектуальной собственности.
3. Вещам.

6 Утверждение «В правовой системе Российской Федерации возможна купля-продажа NFT»:

1. Верно.
2. Не верно.

3. Ответ зависит от вида NFT, передаваемого по договору купли-продажи.

7 Криптовалюта на территории Российской Федерации не может:

1. Приниматься в качестве оплаты товаров, работ и услуг.
2. Быть арестована в качестве имущества в рамках исполнительного производства.
3. Облагаться налогами при совершении операций с ней.

8 Согласно пп. «а» п. 5 Указ Президента РФ от 10.10.2019 N 490 «О развитии искусственного интеллекта в Российской Федерации» искусственный интеллект – это:

1. Комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека.
2. Средства, которые определяют восприимчивость ЭВМ к языкам программирования высокого уровня, близким к естественному языку выдачи заданий на решение задач, а также средств, позволяющих выполнить эти задания за счет знаний о предметной области, где решается данная задача.
3. Передовой машинный интеллект.

9 С помощью использования блокчейн-технологии в юриспруденции возможно:

1. Сократить расходы на бумажный документооборот.
2. Обеспечить необходимый уровень прозрачности сделок.
3. Оба варианта верны.

10 Какие три основные свойства информации достигаются с помощью защиты информации?

1. Актуальность, достоверность, защищенность
2. Отчуждаемость, правильность, упругость
3. Конфиденциальность, целостность, доступность
4. Нет правильного ответа

11 LegalTech представляет собой:

1. Различного рода онлайн-приложения и сервисы, которые позволяют заменить традиционные способы получения юридических услуг новыми и (или) облегчают пользователям доступ к правовой информации.
2. Рынок IT-технологий.
3. Технологические решения, создаваемые для профессиональных юристов и юридического бизнеса с целью повышения эффективности оказания юридических услуг или юридического сопровождения бизнеса.

12 Основные объекты информационной безопасности:

1. Компьютерные сети, базы данных
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы

13 Основными рисками информационной безопасности являются:
1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. Потеря, искажение, утечка информации

14 К основным принципам обеспечения информационной безопасности относится:
1. Экономической эффективности системы безопасности
2. Многоплатформенной реализации системы
3. Усиления защищенности всех звеньев системы

15 Основными субъектами информационной безопасности являются:
1. Руководители, менеджеры, администраторы компаний
2. Органы права, государства, бизнеса
3. Сетевые базы данных, фаерволлы.

16 Справочно-правовые системы – это:
1. Класс компьютерных баз данных, направленных на информационное
сопровождение работы юристов и специалистов смежных профессий.
2. Программное обеспечение для специалистов юридической и смежных специальностей.
3. Необходимое средство в работе с правовой информацией.

17 Каким термином обозначается анализ регистрационной информации системы защиты?
1. Мониторинг
2. Аудит
3. Аккредитация
4. Сертификация

18 «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федераци» по следующим направлениям разработки, апробации и внедрения цифровых инноваций:
1. Медицинская деятельность, в том числе с применением телемедицинских технологий и технологий сбора и обработки сведений о состоянии здоровья и диагнозах граждан, фармацевтическая деятельность.
2. Продажа товаров, работ, услуг дистанционным способом.
3. Все ответы верны.

19 Основным нормативно-правовым актом в области регулирования цифровой экономики является:

1. Федеральный закон от 31.07.2020 N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».
2. "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ.
3. Федеральный закон от 02.08.2019 N 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации».

Критерии оценки:

3-4 балла по шкале БРС выставляется обучающемуся, если даны правильные ответы на 2 вопроса из 2;

1-2 балла по шкале БРС выставляется обучающемуся, если дан правильный ответ на 1 вопрос из 2;

0 баллов по шкале БРС выставляется обучающемуся, если дан правильный ответы на 0 вопросов из 2.

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ К ЛАБОРАТОРНЫМ РАБОТАМ

Контрольные вопросы для защиты лабораторной работы №1.

1. Назовите преимущества закрытого хеширования.
2. Каков принцип построения хеш-таблиц?
3. Почему возможно возникновение коллизий?
4. Каковы методы устранения коллизий? Охарактеризуйте их эффективность в различных ситуациях.
5. Назовите преимущества открытого хеширования.
6. Как выбирается метод изменения адреса при повторном хешировании?

Контрольные вопросы для защиты лабораторной работы №2.

1. Что подразумевается под термином «Одноранговая сеть (P2P)»?
2. Как пользователи узнают о том, что существуют другие пользователи?
3. Как устроена организация сети по блокам?
4. Как проходит проверка данных блокчейна?
5. Опишите алгоритм проверки транзакции?
6. Опишите алгоритм проверки блока?
7. Кто проверяет данные блокчейна?

Контрольные вопросы для защиты лабораторной работы №3.

1. Можно ли использовать обычный метод сжатия без потерь, например ZIP, в роли криптографической хэш-функции?
2. Можно ли использовать функцию контрольной суммы как криптографическую хэш-функцию?
3. Дайте определение термину «хеш-код».
4. Назовите недостатки открытого хеширования.
5. Назовите недостатки закрытого хеширования.
6. Дайте определение термину «хеш-сумма».
7. Дайте определение термину «хэш-функция».
8. Что означает стойкость хэш-функции к коллизиям?

Контрольные вопросы для защиты лабораторной работы №4.

1. Будет ли стойкая к коллизиям функция обязательно односторонней?
2. Для каких целей используются хеш-функции?
3. Перечислите основные требования, предъявляемые к хеш-функциям.
4. Назовите примеры криптографических хеш-функций.
5. Каков российский стандарт на алгоритм формирования криптографической хеш-функции?
6. Каким образом можно использовать блочный алгоритм шифрования для формирования хеш-функции?

Контрольные вопросы для защиты лабораторной работы №5.

1. Что такое майнинг?
2. Дайте определение термину «Целостность».
3. Кто такой майнер?
4. Дайте определение термину «Прозрачность».
5. Что такое смарт-контракты?
6. В чем разница между секьюрити и ютилити токенами?
7. Дайте определение термину «Децентрализация».

Критерии оценки:

4 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1-2 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.4 ВОПРОСЫ К САМОСТОЯТЕЛЬНЫМ РАБОТАМ

Контрольные вопросы для самостоятельной работы №1.

1. В какой стране впервые велись работы по распределённым вычислениям?
2. Для каких нужд разрабатывались первые распределенные реестры?
3. Назовите цели построения РВС
4. Дайте определение термину «Отказоустойчивость».
5. Дайте определение термину «Географически распределенная вычислительная среда».
6. Что вы знаете об ARPANET?

Контрольные вопросы для зсамостоятельной работы №2.

1. Что такое "Облачная" технология вычислений?
2. Как построена грид-технология построения сети?
3. Какая архитектура у одноранговой сети?
4. Что такое «Распределенные вычислительные системы»?
5. Какие виды РВС вы знаете?
6. Какие недостатки имеет архитектура P2P?

Контрольные вопросы для самостоятельной работы №3.

1. Каковы преимущества распределенных вычислений?
2. РВС имеет возможность масштабирования? Если да, обоснуйте.
3. К свойствам РВС можно отнести «Доступность»? Если да, обоснуйте.
4. «Согласованность» является качеством РВ систем?
5. Можно ли назвать РВ системы прозрачными?
6. «Эффективность» одно из главных преимуществ РВ систем?

Контрольные вопросы для самостоятельной работы №4.

1. Какие рекомендации по безопасной настройке блокчейн-платформы вы можете дать?
2. Каковы процессы разработки и тестирования блокчейн решения?
3. Как решены вопросы доверия к внешним данным, записываемым в блокчейн?
4. Назовите атаки на используемые алгоритмы консенсуса?
5. Какова криптостойкость известных криптографических алгоритмов?
6. Кто в распределенной системе отвечает за ИБ?
7. Необходимы ли проверки защищенности узлов сети?

Контрольные вопросы для самостоятельной работы №5.

1. Назовите элементы эксплуатации межсетевого взаимодействия.
2. Расскажите регламент и последовательность установления взаимодействия.
3. Назовите основные проблемы приема межсетевой информации?
4. Опишите разграничение доступа к конфиденциальной информации.
5. Назовите типовой порядок действий при переконфигурации сети ViPNet.
6. Как осуществляется разбиение сети ViPNet на самостоятельные подсети.
7. Как осуществляется контроль правильности конфигурации системы?

Контрольные вопросы для самостоятельной работы №6.

1. Назовите элементы эксплуатации межсетевого взаимодействия.
2. Расскажите регламент и последовательность установления взаимодействия.
3. Назовите основные проблемы приема межсетевой информации?
4. Опишите разграничение доступа к конфиденциальной информации.
5. Назовите типовой порядок действий при переконфигурации сети ViPNet.
6. Как осуществляется разбиение сети ViPNet на самостоятельные подсети.
7. Как осуществляется контроль правильности конфигурации системы?

Контрольные вопросы для самостоятельной работы №7.

1. Что такое Linux и основные компоненты?
2. Что такое ядро Linux?
3. Что такое inode в Linux? Как найти индекс, связанный с файлом?
4. Как искать файлы в linux?
5. Как создать пользователя и группу в Linux?
6. Как найти версию ядра / ОС в Linux?
7. Кэш и буфер на Linux.

Контрольные вопросы для самостоятельной работы №8.

1. Что понимается под «сетевым мультимедиа» для РВС?
2. Назовите элементы дифференцированные службы для РВС.
3. Система «виртуальной лаборатории».

4. Реализация тактильной и силовой обратной связи в РВС.
5. Проблема задержки и ее нестабильности в рамках сетевого мультимедиа.
6. Особенности трафика тактильной информации.
7. Особенности трафика силовой информации.

Критерии оценки:

1 балл выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0.5 балла выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Какой класс систем является наиболее представительным (большим)?

   a. распределенные системы

   b. децентрализованные системы.

   c. блокчейны

   d. криптовалюты

2. Для каких сфер бизнеса следует использовать блокчейн?

   a. в облачных вычислениях

   b. в производстве потребительских товаров

   c. в схемах, основанных на публичных реестрах

   d. в децентрализованном учете и взаиморасчетах

3. В иерархии децентрализованных распределенных систем блокчейнам непосредственно предшествует класс …

   a. распределенных систем

   b. централизованных систем

   c. децентрализованных систем

   d. криптовалют

4. Децентрализованные приложения …

   a. расширяют возможности сети Интернет

   b. сужают возможности сети Интернет

   c. работают независимо от сети Интернет

   d. не изменяют возможности сети Интернет

5. Наличие единого, центрального сервера, копирующего свои данные на вспомогательные серверы, говорит о том, что …

   a. в системе не используется блокчейн

   b. в системе используется частный блокчейн

   c. мы имеем дело с распределенной базой данных

   d. в системе используется публичный блокчейн

6. Для каких сфер бизнеса не следует использовать блокчейн?

   a. анализ данных

   b. внутренний документооборот компании

   c. децентрализованная торговля

   d. голосование

7. Укажите основные тренды цифровой экономики, проявившие себя в технологии блокчейн:

   a. формируется на стыке нескольких разнонаправленных видов деятельности, науки, экономики

   b. способствует локализации бизнес-деятельности

   c. исключает посредников

d. существенным образом зависит от человеческого фактора

8. Укажите виды деятельности, благоприятные для внедрения систем на основе блокчейнов:

a. бизнес-процессы с очень высокой интенсивностью трафика (информационных потоков)

b. системы с высокой конфиденциальностью, например, финансовые отчеты коммерческих предприятий (корпораций)

c. регистрация актов гражданского состояния

d. кадастровая деятельность

9. Укажите препятствия на пути развития технологии блокчейн:

a. малая пропускная способность сети

b. постоянное увеличение размера физического хранилища, в котором хранится цепочка блоков

c. саботаж пользователей

d. слабая поддержка со стороны производителей аппаратного обеспечения

10. Можно ли утверждать, что правовые аспекты применения технологии блокчейх плохо отрегулированы?

a. Да

b. Нет

11. Является ли точным и корректным определение "блокчейн - распределенная база данных"?

a. Да

b. Нет

12. Применение технологии блокчейн в любых сферах будет экономически выгодным и технологически оправданным?

a. Да

b. Нет

13. Технология блокчейн устраняет следующий недостаток современных бизнес-процессов …

a. наличие посредников

b. невысокая скорость финансовых операций

c. трансакционные издержки

d. неразвитость информационной инфраструктуры

14. Технология блокчейн обеспечивает …

a. автоматизацию бизнес-процесса

b. трансформацию бизнес-процесса

c. механизацию бизнес-процесса

d. информатизацию бизнес-процесса

15. Кому именно приписывают создание протокола Биткоин?

a. Билл Гейтс

b. Сатоши Накамото

c. Питер Нортон

d. Марк Цукерберг

16. Какую задачу впервые удалось решить с помощью платформы Биткоин?

a. двойных трат

b. анонимности платежей

c. электронных платежей

d. масштабируемости платежных систем

17.Дефляционный характер криптовалюты Биткоин объясняется …

a. виртуальным характером монет

b. отсутствием центрального, управляющего звена

c. строго ограниченным числом монет, подлежащих выпуску

d. высокой волатильностью курса

18.В сети Биткоин полностью открыты …

a. протокол Биткоин и программный код базового клиента Bitcoin Core

b. только протокол Биткоин

c. только программный код базового клиента Bitcoin Core

d. только API (Application Programming Interface - интерфейс программных приложений) функции

19.Можно ли менять данные в блокчейне?

a. Да

b. Нет

20.Может ли уменьшаться число блоков в блокчейне?

a. Да

b. Нет

21. Можно ли нарушать хронологический порядок при добавлении блоков?

a. Да

b. Нет

22. В каких блокчейнах генерация новых блоков осуществляется централизованным образом?

a. приватных

b. публичных

c. сайдчейнах

d. стейблкоинах

23. Достоинством закрытых блокчейнов является …

a. прозрачность данных и процессов

b. полный контроль над системой со стороны всех ее участников

c. потенциально высокая пропускная способность системы

d. повышенный уровень безопасности и надежности системы

24. Достоинством открытых блокчейнов является …

a. высокий уровень доверия со стороны пользователей

b. низкая стоимость транзакций

c. высокая скорость подтверждения транзакций

d. более контролируемая и прогнозируемая среда для реализации бизнес-функций

25. С помощью какого средства осуществляется управление биткоинами?

a. криптографических ключей

b. кредитных карт

c. банковских счетов

d. токенов

26. Что является необходимым и достаточным условием для работы с платежной системой Биткоин?

a. наличие биткоинов

b. наличие фиатных денег

c. наличие установленного клиента сети Биткоин

d. наличие аккаунта на криптовалютной бирже

27. Биткоин является …

a. одноранговой платежной системой

b. платежной системой с процессинговыми центрами

c. многополярной платежной системой

d. клиент-серверной платежной системой

28. Для достижения консенсуса в сети Биткоин используется механизм?

a. Proof of Work

b. Proof of Stake

c. Proof of Capacity

d. Proof of Activity

29. С помощью какого инструмента обеспечивается высочайшая отказоустойчивость сети Биткоин?

a. сеть Интернет

b. управляющие центры

c. децентрализация

d. прозрачность взаимодействия

30. Перевод средств в сети Биткоин считается завершенным …

a. только после включения в блокчейн нового блока с соответствующей транзакцией

b. сразу после завершения операции в программе-клиенте пользователя

c. после отправки соответствующей транзакции в сеть

d. по прошествии 12-ти часового периода времени

31. Кто занимается сборкой блоков в сети Биткоин?

a. майнеры

b. администраторы

c. все пользователи сети

d. блокировщики

32. Временной интервал между двумя блоками в блокчейне сети Биткоин составляет в среднем …

a. 1 минуту

b. 5 минут

c. 10 минут

d. 30 минут

33. Каким образом в каждом новом блоке учитывается вся предыстория блокчейна, включая блок генезиса?

a. путем вставки в новый блок ссылки на хеш предыдущего блока

b. путем электронного подписания каждого нового блока

c. путем нумерации блоков

d. путем вставки в новый блок ссылок на все предыдущие блоки

34. Назовите основные характеристики блокчейна.

a. технология криптозащиты

b. учетный журнал

c. строго хронологический порядок записей

d. система сбора и хранения данных

35. Что такое биткоин?

a. криптоключ

b. цифровой актив

c. тип кредитной карты

d. криптовалюта

36. В каких случаях можно использовать биткоин?

a. для хранения ценностей

b. для совершения электронных оплат

c. для пополнения бумажных счетов

d. для покупки услуг

37.Какой из примеров можно отнести к одноранговому типу общения?

a. онлайн отправка денег другому лицу

b. отправка письма через интернет другому лицу

c. перевод денег с помощью организации-посредника

d. отправка письма через почтовое отделение

38.Что такое блокчейн?

a. глобальная сеть с тысячами компьютеров

b. особо децентрализованный учетный журнал

c. ключевая технология, содержащая децентрализованную запись транзакций

d. централизованная база данных, подтверждающая проведение сделки

39.Назовите основные задачи майнеров?

a. обработка и подтверждение транзакций

b. решение криптографических задач

c. децентрализованное размещение данных по каждой сделке

d. создание цепи записей, которые формируют учетный журнал биткойн

40.Что такое хэш?

a. криптографически зашифрованная сделка

b. цифровой отпечаток определенного набора данных

c. децентрализованное разрешение криптографических задач

d. объем данных в алфавитно-цифровом формате определенной длины

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

a. по мере обработки майнерами

b. каждые десять минут

c. раз в сутки

d. после 100% заполнения нового блока

42. Назовите вид хеш-функции, которая используется в Биткойн.

a. SHA256

b. HAS265

c. SAH256

d. SHA265

43. Чем криптовалюта отличается от традиционных валют?

a. у криптовалют нет материальных денег

b. криптовалюты отправляются другому лицу без посредников

c. у криптовалют нет бумажных счетов

d. криптовалюта не может быть использована для хранения ценностей

44.Каким образом подтверждается сделка в сети биткоин между людьми?

a. банком

b. централизованным хранилищем

c. клиринговой организацией

d. технологией блокчейн

45.Каким образом технология блокчейн защищена от возможности единой ошибки?

a. криптографические коды

b. децентрализованное хранение данных в сети

c. единое централизованное хранение данных

d. транзакционное подтверждение третьими лицами

46.Назовите главное отличие между хешированием и шифрованием.

a. уникальный цифровой отпечаток шифра не может быть возвращен к исходному тексту

b. хеш позволяет вернуться к исходному тексту без ключа

c. хеш является односторонней функцией

d. шифр имеет ограничения по обработке объема данных

47.Из каких чисел составляется блок?

a. данные

b. математический шифр

c. криптографический хеш

d. одноразовый номер

48. В каком случае блок может быть признан действительным и включен в блокчейн?

a. если для решения криптографической задачи был задействован 51% технического обеспечения

b. если майнеры использовали единое программное обеспечение для решения криптографической задачи

c. если найден одноразовый номер для конкретной криптографической задачи

d. если криптографическая задача была решена менее чем за 10 минут

49. Назовите элемент, который является общим для каждого блока.

a. номер

b. объем данных

c. сопутствующий хэш

d. PREV

50. Когда система высчитывает действующий хэш?

a. при хронологическом выстраивании блоков

b. при создании криптографического хэша

c. во время добычи блока

d. при возврате к исходному количеству символов

51. Назовите основные составляющие биткоин.

a. программное обеспечение

b. криптографическое испытание

c. майнеры

d. централизованное хранилище

52. Закрытые криптографические ключи в сети Биткоин …

a. выдаются в удостоверяющих центрах

b. генерируются и хранятся в кошельках

c. распространяются по сети

d. хранятся в блокчейне

53. Для управления закрытыми криптографическими ключами в сети Биткоин …

a. нужно обращаться к администратору сети

b. достаточно иметь кошелек

c. используют криптопровайдер КриптоПро

d. используется блокчейн

54. Закрытый криптографический ключ в сети Биткоин – это …

a. число

b. кодовое слово

c. механическое устройство

d. комбинация цифр и символов

55. Какой тип криптографии используется в платформе Биткоин?

a. симметричная

b. асимметричная

c. гибридная

d. стеганография

56. Если y = f(x) – односторонняя функция, тогда …

a. вычислить x, зная y, невозможно в принципе

b. вычислить x, зная y, очень сложно

c. вычислить y, зная x, очень сложно

d. вычислить y, зная x, невозможно в принципе

57. Какие ключи используются в криптосистеме с закрытым ключом …

a. открытые и закрытые

b. симметричные

c. сеансовые

d. коды аутентичности

58. Если проводить аналогию между банковским чеком и транзакцией сети Биткоин, с каким реквизитом чека можно ассоциировать биткоин-адрес?

a. имя получателя средств

b. название банка

c. номер банковского счета

d. подпись на банковском чеке

59. С каким элементом традиционной платежной системы ассоциируется закрытый ключ платформы Биткоин?

a. пин-кодом банковской карты

b. номером банковского счета

c. именем получателя средств

d. личным кабинетом пользователя на сайте платежной системы

60. С каким элементом традиционной платежной системы ассоциируется открытый ключ платформы Биткоин?

a. номером банковского счета

b. пин-кодом банковской карты

c. подписью на банковском чеке

d. банковской ячейкой

61. В сети Биткоин для создания криптопары используется …

a. умножение на эллиптических кривых

b. деление на эллиптических кривых

c. логарифмирование на эллиптических кривых

d. вычитание на эллиптических кривых

62. Длина закрытого ключа составляет …

a. 256 бит

b. 512 бит

c. 128 бит

d. 1024 бита

63. Укажите правильную последовательность вычислений …

a. закрытый ключ → открытый ключ → биткоин-адрес

b. биткоин-адрес → закрытый ключ→ открытый ключ

c. открытый ключ → закрытый ключ → биткоин-адрес

d. закрытый ключ → биткоин-адрес → открытый ключ

64. Укажите правильную формулу для вычисления биткоин-адреса

a. SHA-256(RIPEMD-160(публичный ключ)

b. SHA-256(SHA-256 (публичный ключ)

c. RIPEMD-160(RIPEMD-160(публичный ключ)

d. RIPEMD-160(SHA-256(публичный ключ)

65. Закрытый ключ …

a. вычисляется как точка на эллиптической кривой

b. берется из справочника

c. вычисляется случайным образом

d. берется из блокчейна

66. С помощью закрытого ключа создается

a. электронная подпись

b. кошелек

c. биткоины

d. блок

67. Можно ли восстановить доступ к средствам в сети Биткоин после потери закрытого ключа?

a. Да

b. Нет

68. Может ли кто-то, кроме владельца закрытого ключа, контролировать средства, связанные с соответствующим биткоин-адресом?

a. Да

b. Нет

69. Можно ли подбросив 256 раз монету и записав результаты опытов в виде последовательности нулей и единиц получить правильный закрытый ключ?

a. Да

b. Нет

70. В чем именно состоит недостаток традиционных (не квантовых) генераторов случайных чисел?

a. недостаточно высокая неопределенность вычислений

b. не позволяют генерировать большие числа

c. медленно работают

d. дорого стоят

71. Какие генераторы случайных чисел являются самыми лучшими (надежными)

a. физические

b. табличные

c. квантовые

d. алгоритмические

72. Какие генераторы случайных чисел используются в сети Биткоин?

a. штатные генераторы случайных чисел, входящие в состав операционных систем

b. квантовые генераторы

c. табличные генераторы

d. физические генераторы

73. В эллиптической криптографии закрытый ключ можно получить из открытого ключа только …

a. путем перебора всех возможных значений (brute force)

b. применяя эксплойтинг

c. применяя SQL-инъекции

d. используя алгоритмы имитационного моделирования

74. Криптография на эллиптических кривых основана на

a. проблеме дискретного логарифмирования на эллиптических кривых

b. использовании нескольких раундов шифрования с разными ключами

c. сложности криптоанализа при использовании объемной (многомерной) перестановки

d. сложности криптоанализа при использовании усовершенствованного метода многозначной замены

75. Укажите параметры криптографического алгоритма сети Биткоин:

a. простой модуль

b. базовая точка

c. скорость схождения

d. длина кодового слова

76. Укажите основные свойства эллиптических кривых, используемые в криптографии:

a. дискриминант уравнения эллиптической кривой не равен нулю.

b. свойство делимости точек эллиптических кривых над конечным полем

c. любая наклонная прямая, пересекающая эллиптическую кривую в двух точках, всегда будет пересекать ее также в третьей точке

d. любая наклонная прямая, являющаяся касательной к кривой в одной из точек, обязательно пересечет кривую еще ровно в одной точке

77. Какие операции на эллиптических кривых используются в криптографии платформы Биткоин?

a. сложение

b. деление

c. умножение

d. вычитание

78. Что является результатом скалярного умножения на эллиптических кривых базовой точки на значение закрытого ключа?

a. точка на эллиптической кривой

b. целое число

c. вещественное число

d. прямая линия, пересекающая эллиптическую кривую

79. Эллиптическая кривая симметричная относительно …?

a. ось ординат

b. начала координат

c. оси абсцисс

d. диагонали декартовой системы координат, пересекающей ее в I и III четвертях

80. В протоколе Биткоин базовая точка …

a. однозначно определена и зафиксирована

b. является случайной

c. задается для каждого пользователя индивидуально

d. меняется после добавления в блокчейн определенного числа блоков

81. Выберите из списка этапы жизненного цикла транзакции в сети Биткоин:

a. подписание электронной подписью

b. проверка и включение в блок майнером

c. микширование

d. подсчет статистики

82. Какие элементы платежа, реализованного с помощью транзакции сети Биткоин, роднят его с банковским чеком?

a. транзакции проверяются майнерами

b. транзакции объединяются в блоки

c. транзакции подписываются непосредственно владельцами средств

d. транзакции содержат ссылки на средства других транзакций (счетов)

83. Прозрачность блокчейна в том числе заключается в том, что …

a. каждый пользователь сети Биткоин всегда может отследить любую цепочку транзакций, фиксирующих движение конкретных биткоинов

b. каждый пользователь сети Биткоин может внести изменения в блокчейн

c. каждый пользователь сети Биткоин может анализировать транзакции (сделки), которые еще даже не включены в блоки

d. каждый пользователь сети Биткоин может определить персональные данные других участников сети

84. Что означает правило шести подтверждений?

a. каждую транзакцию должны подтвердить шесть майнеров

b. чтобы считать сделку завершенной, следует дождаться включения в блокчейн шести дополнительных блоков (подтверждений).

c. дерево Меркла в блоке должно иметь не менее шести ветвей

d. каждый блок должны подтвердить шесть майнеров

85. Что представляет собой атака Сивиллы?

a. под контролем злоумышленника оказывается более 50% хешрейта

b. узел-жертва ограничена коммуникациями только с узлами, контролируемыми злоумышленником

c. отправка большого количества «мусорных» данных (транзакции-спам) на узел пользователя

d. взлом хэш-функций

86. Анонимность расчетов в сети Биткоин …

a. ограничена исключительно рамками сети Биткоин

b. не обеспечивается даже в рамках сети Биткоин

c. распространяется на все финансовые институты, включая криптовалютные биржи

d. невозможна в принципе

87. Можно ли для отправки транзакций использовать такие незащищенные средства как Wi-Fi или Bluetooth?

a. Да

b. Нет

88. Можно ли для отправки транзакций использовать каналы спутниковой или коротковолновой радиосвязи?

a. Да

b. Нет

89. Проверяет ли каждый активный узел все полученные по сети транзакции?

a. Да

b. Нет

90. Основной формой реализации транзакций в сети Биткоин являются …

a. P2SH-транзакции

b. P2PKH-транзакции

c. мультиподписные транзакции

d. P2PK-транзакции

91. Для разблокирования средства на выходе P2PKH-транзакции …

a. достаточно предъявить открытый ключ владельца средств

b. необходимо предъявить открытый ключ и электронную подпись владельца средств

c. достаточно предъявить электронную подпись владельца средств

d. необходим PIN-код к биткоин-адресу, на который были посланы средства

92. Биткоин-адрес P2SH-транзакции, записанный в кодировке Base58Check, начинается с цифры …

a. 3

b. 1

c. 2

d. 4

93. Какой тип транзакций в сети Биткоин позволяет реализовать схему платежа, в которой разблокирующий сценарий известен только получателю средств …

a. P2SH-транзакции

b. P2PKH-транзакции

c. транзакции выход данных (OP_RETURN)

d. P2PK-транзакции

94. В случае с P2SH-платежом какая сторона сделки экономит на комиссионных майнерам больше?

a. получателя

b. отправителя

c. расходы делятся поровну между отправителем и получателем

d. в P2SH-транзакции вообще не предусмотрены комиссионные

95. Какой тип транзакции реализует сценарий мульти-подписного адреса?

a. P2SH

b. P2PKH

c. P2PK

d. выход данных (OP_RETURN)

96. Какой максимально возможный по числу участников в сценарии мульти-подписи вариант реализован в сети Биткоин?

a. 25-из-25

b. 15-из-15

c. 10-из-05

d. 5-из-5

97. Что хранится в пуле UTXO?

a. биткоины

b. неизрасходованные выходы транзакций

c. данные пользователей

d. цепочка блоков

98. Что является недостатком модели UTXO?

a. плохо работает в предметных областях, где на один актив претендуют сразу несколько владельцев

b. не подходит для децентрализованных приложений

c. плохо доказуема с точки зрения теоретической информатики

d. плохо работает в криптовалютах

99. Поддерживает ли протокол Биткоин такой элемент платежных систем как балансовый счет?

a. Да

b. Нет

100. Содержит ли блокчейн сети Биткоин данные о владельцах средств?

a. Да

b. Нет

Задания в открытой форме

1) … — это общая база данных в блокчейн-сети, в которой хранятся копии транзакций (например, в виде редактируемого всеми участниками общего файла).

2) … - это постоянно растущий учетный журнал, который ведет постоянную запись всех сделок, которые имели место в безопасном, хронологическом и неизменном порядке.

3) … — это программы в блокчейн-системе, автоматически запускающиеся при соблюдении заданных условий.

4) Внутри сети биткоин существует группа людей, которая называется …, и их роль - обрабатывать и подтверждать транзакции.

5) … содержит весь путь к самой первой сделке в биткоин, которая рассматривается как блок генезиса.

6) Роль … - создавать цепь записей, которые формируют учетный журнал биткоин.

7) Так как биткоин - криптовалюта, и в криптовалюте … - ключевой компонент.

8) … контракты - способ для компьютеров совершать тип взаимодействия, который может требоваться в каком-либо контракте или

соглашении, и можно совершить сделку через компьютер способом, который сокращает посредников, автоматизирован, самоисполняем и неизменен.

9) … — исторически первое и наиболее известное применение блокчейн-технологии.

10) Некоторые типы блокчейна потенциально уязвимы перед хакерскими атаками, а также перед так называемыми «…» — когда, в полном соответствии с правилами системы, коалиция пользователей, обладающих большими компьютерными мощностями, может изменить записи в конкретном блокчейне.

11) Компании используют … для самостоятельного управления коммерческими сделками без привлечения третьей стороны.

12) Криптография с открытым ключом — это система безопасности, позволяющая однозначно … участников блокчейн-сети.

13) … отражает перемещение физических или цифровых активов от одной стороны к другой в блокчейн-сети.

14) … действует как цепочка, связывающая блоки вместе.

15) … блокчейны не требуют разрешений и позволяют любому желающему присоединиться к сети.

16) … блокчейны, которые также можно назвать управляемыми, контролируются одной организацией.

17) … блокчейн сочетает в себе функции как частных, так и публичных сетей.

18) …-консорциумами управляет группа организаций

19) … (крпитовалюта) – это децентрализованная блокчейн-платформа с открытым исходным кодом, используемая для создания публичных блокчейн-приложений. … Enterprise предназначен для коммерческого использования.

20) В публичной сети Bitcoin участники получают … через майнинг — процесс решения криптографических уравнений для создания новых блоков.

Задание на установление правильной последовательности

1. Установить этапы работы блокчейна:

1) Подтвержденная транзакция добавляется в общую «цепь блоков»;

2) Информация о транзакции передается каждому участнику системы блокчейн;

3) Деньги переведены от пользователя А пользователю В.

4) Участники системы подтверждают транзакцию;

5) Пользователь А отправляет монеты пользователю В;

6) Запись данных о транзакции — Информация о транзакции представляется в виде «блока»;

2. Установить хронологию эволюции блокчейн:

1) Стюарт Хабер и Скотт Сторнетта работают над первым блокчейном.
2) Сатоши Накамото выпускает документацию по биткойну.
3) Имеет место первая покупка биткойна в 10000 BTC.
4) Виталик Бутерин выпускает докумен-тацию по Ethereum.
5) Блокчейн Ethereum финансируется при помощи краудсейл.
6) Ethereum предстаяет второй блокчейн.
7) Linux Foundation представляет Гиперледжер для улучшения разработки блокчейнов.
8) EOS.IO представлен block.one как новый протокол блокчейн для развертывания децентрализованных приложений.
9) Технология блокчейн продолжает развиваться. Это представлено ростом числа криптовалют, а также компаниями, использующими эти технологии для повышения эффективности.

3. Установить этапы развития технологии блокчейн:

1) Смарт-контракты;
2) Использование в индустрии;
3) Криптовалюты;
4) Децентрализованные приложения;

4. Установить последовательность представленных этапов блокчейна:

1) Сатоши Накамото выпускает документацию по биткойну.
2) Виталик Бутерин выпускает докумен-тацию по Ethereum.
3) Блокчейн Ethereum финансируется при помощи краудсейл.
4) Ethereum предстаяет второй блокчейн.

5. Установите представленные этапы работы блокчейна в правильной последовательности:

1) Запись данных о транзакции — Информация о транзакции представляется в виде «блока»;
2) Информация о транзакции передается каждому участнику системы блокчейн;
3) Подтвержденная транзакция добавляется в общую «цепь блоков»;
4) Участники системы подтверждают транзакцию;

6. Установить последовательность представленных этапов блокчейна:

1) Стюарт Хабер и Скотт Сторнетта работают над первым блокчейном.

2) Linux Foundation представляет Гиперледжер для улучшения разработки блокчейнов.

3) EOS.IO представлен block.one как новый протокол блокчейн для развертывания децентрализованных приложений.

4) Технология блокчейн продолжает развиваться. Это представлено ростом числа криптовалют, а также компаниями, использующими эти технологии для повышения эффективности.

7. Установите последовательность этапов работы по обеспечению информационной безопасности:

1) Определение требований к системе защиты информации;

2) Выбор контрмер, обеспечивающих режим иб, и средств защиты;

3) Разработка, внедрение и организация использования выбранных мер, способов и средств защиты;

4) Осуществление текущего контроля целостности информационных ресурсов и средств защиты и плановый аудит системы управления информационной безопасностью.

8. Установите этапы развития информационных технологий:

1) «электрическая» технология.

2) «электронная» технология.

3) «компьютерная» технология.

4) «ручная» технология.

5) «механическая» технология.

9. Установить последовательность представленных этапов блокчейна:

1) Имеет место первая покупка биткойна в 10000 BTC.

2) Виталик Бутерин выпускает докумен-тацию по Ethereum.

3) Блокчейн Ethereum финансируется при помощи краудсейл.

4) Технология блокчейн продолжает развиваться. Это представлено ростом числа криптовалют, а также компаниями, использующими эти технологии для повышения эффективности.

10. Расположите этапы развития информационных технологий в соответствии с проблемами, стоящими на пути информатизации общества.

1) Максимальное удовлетворение потребностей пользователя и создание соответствующего интерфейса работы в компьютерной среде.

2) Обработка больших объемов данных в условиях ограниченных возможностей аппаратных средств.

3) Отставание программного обеспечения от уровня развития аппаратных средств.

4) Выработка соглашений и установление стандартов, протоколов для компьютерной связи; организация доступа к стратегической информации; организация защиты и безопасности информации.

11. Процесс разработки блокчейна включает в себя следующие этапы:

1) Сопровождение
2) Модификация
3) Программирование
4) Анализ
5) Проектирование

12. Выберите правильную последовательность этапов разработки профиля защиты.

1) Анализ среды применения ИТ-продукта с точки зрения безопасности.
2) Выбор профиля-прототипа.
3) Синтез требований.

13. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:

1) Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
2) Реализация защитных мер по противодействию скрытых каналов
3) Организация контроля за противодействием скрытых каналов.
4) Выявление скрытых каналов и оценка их опасности для активов организации

14. Выберите последовательность приоритетных этапов защиты информации:

1) Защита информации от несанкционированного доступа;
2) Защита информации в системах связи;
3) Защита юридической значимости электронных документов;
4) Защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;
5) Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;
6) Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

15. Выберите правильную последовательность этапов работы по обеспечению ИБ:

1) Выявление максимально полного множества потенциальных угроз, способов и каналов их осуществления;
2) Определение и выработка политики информационной безопасности;
3) Определение совокупности целей создания системы иб и сферы (границ) ее функционирования;
4) Выявление уязвимостей, проведение оценки рисков, формирование методик управление рисками;
5) Выберите правильную последовательность этапов работы по обеспечению режима ИБ:

16. Установите последовательность этапов работы по обеспечению информационной безопасности:
1) Определение требований к системе защиты информации;
2) Выбор контрмер, обеспечивающих режим иб, и средств защиты;
3) Разработка, внедрение и организация использования выбранных мер, способов и средств защиты;
4) Осуществление текущего контроля целостности информационных ресурсов и средств защиты и плановый аудит системы управления информационной безопасностью.

17. Выберите правильную последовательность этапов процесса управления рисками:
1) Идентификация активов и ценности ресурсов, нуждающихся в защите;
2) Анализ угроз и их последствий, определение слабостей в защите;
3) Классификация рисков, выбор методологии оценки рисков и проведение оценки;
4) Выбор, реализация и проверка защитных мер;
5) Оценка остаточного риска;
6) Выбор анализируемых объектов и степени детальности их рассмотрения;

18. Выберите правильную последовательность этапов разработки блокчейн проекта:
1) Оценка стоимости;
2) Реализация политики;
3) Квалифицированная подготовка специалистов;
4) Разработка политики безопасности;

19. Выберите последовательность уровней безопасности информации:
1) Административный уровень
2) Процедурный уровень
3) Программно-технический уровень

4) Законодательный уровень

20. Выберите правильную последовательность этапов построения политики безопасности:

1) Выбор и установка средств защиты;

2) Организация обслуживания по вопросам информационной безопасности;

3) Создание системы периодического контроля информационной безопасности

4) Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;

5) Подготовка персонала работе со средствами защиты;

Задание на установление соответствия

1. Установить соответствие основных уровней блокчейн сетей:

1) Блокчейн 1.0	a) Криптовалюты
2) Блокчейн 2.0	b) Смарт-контракты
3) Блокчейн 3.0	c) Децентрализованные приложения
4) Блокчейн 4.0	d) Использование в индустрии

2. Установить соответствие основных уровней блокчейн сетей:

1) 0 уровень L0	a) Polkadot.
2) 1 уровень L1	b) Bitcoin.
3) 2 уровень L2	c) Polygon.
4) 3 уровень L3	d) Uniswap.

3. Установить соответствие основных уровней блокчейн сетей:

1) 0 уровень L0	a) Avalanche.
2) 1 уровень L1	b) Ethereum.
3) 2 уровень L2	c) Optimism.
4) 3 уровень L3	d) PancakeSwap.

4. Установить соответствие основных уровней блокчейн сетей:

1) 0 уровень L0	a) Cosmos.
2) 1 уровень L1	b) TON.
3) 2 уровень L2	c) Arbitrum.
4) 3 уровень L3	d) Curve.

5. Установить соответствие нарушителей по уровням возможностей (используемым методам и вопросам):

1) 1 уровень	a) Применяющие пассивные средства (технические средства перехвата без модификации компонентов системы).
2) 2 уровень	b) Применяющие только агентурные методы получения сведений
3) 3 уровень	c) Использующие только штатные средства и недостатки системы защиты, их сильные и слабые стороны.
4) 4 уровень	d) Применяющие методы и действия активного воздействия (модификация и подключение дополнительных технических устройств).

6. Установить соответствие основных узлов блокчейн:

1) Сетка	a) узел (нода) коннектиться к каждому другому узлу.
2) Кольцо	b) узел соединяется с двумя другими узлами, создавая двунаправленное кольцо.
3) Шина	c) серверный узел коннектиться с клиентскими узлами.
4) Звезда	d) узел соединяется только с одним другим узлом.

7. Установить соответствие:

1) Public blockchain	a) это блокчейн, в котором процесс согласования контролируется заранее выбранным набором узлов.
2) Consortium blockchain	b) это цепочка блоков, которую может «прочитать» любой человек в мире.
3) Fully private blockchain	c) это блокчейн, характеризующийся ограниченным уровнем доступа к данным.

8. Установить соответствие:

1) OLE-automation или просто Automation	a) Технология, организующая доступ к данным разных компьютеров с учетом балансировки нагрузки сети.
2) ActiveX	b) Технология, обеспечивающая безопасность и стабильную работу распределенных приложений при больших объемах передаваемых данных.
3) MIDAS	c) Технология предназначена для создания программного обеспечения как сосредоточенного на одном компьютере, так и распределенного в сети.
4) MTS (Microsoft Transaction Server)	d) Технология создания программируемых приложений, обеспечивающая программируемый доступ к внутренним службам этих приложений

9. Установить соответствие основных видов реестров:

1) Unpermissioned public ledgers	a) открытые публичные реестры.
2) Permissioned public ledgers	b) закрытые публичные реестры.
3) Permissioned private ledgers	c) закрытые частные реестры

10. Установить соответствие:

1) Планирование	a) Отладка программы в соответствии с индивидуальными запросами конкретного предприятия базируется на контроле конфиденциальных сведений в соответствии с признаками особенной документации, принятой в компании
2) Реализация	b) Заключается в точном определении программы защиты данных. Ответ на простой, казалось бы, вопрос: «Что будем защищать?»
3) Корректировка	c) Проанализировав информацию, собранную на этапе тестовой эксплуатации DLP-решения, приступают к перенастройке ресурса.

11. Установить соответствие уровней технологий блокчейн:

1) Уровень приложений	a) В этом разделе вы получите доступ ко всем основным инструментам, которые помогут вам создать и запустить уровень dApps.
2) Уровень услуг	b) Он поставляется с dApps, браузером dApp, пользовательским интерфейсом и хостингом приложений.
3) Семантический уровень	c) На этом уровне присутствуют консенсусные алгоритмы, виртуальные машины, любые требования к участию и так далее.

12. Установить соответствие:

1) Угроза целостности	a) Это вероятный ущерб, который зависит от защищенности системы.
2) Угроза доступности	b) Это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или

	доступности по каждому виду ценной информации.
3) Ущерб	c) Это угроза нарушения работоспособности системы при доступе к информации.
4) Риск	d) Это угроза изменения информации.

13. Установить соответствие:

1) Системность целевая	a) Подразумевает единство организации всех работ по защите информации и их управления.
2) Системность пространственная	b) Защищенность информации рассматривается как составная часть общего понятия качества информации.
3) Системность временная	c) Защищенность основанная на принципе непрерывности функционирования системы защиты
4) Системность организационная	d) Защищенность рассматривается как увязка вопросов защиты информации

14. Установить соответствие средств информационной защиты:

1) SIEM-системы	a) Виртуально-частная сеть определяет использование собственной частной сети внутри общедоступной. Поэтому ваше приложение, работающее по VPN, будет надежно защищено.
2) CloudAV	b) Они собирают информацию о возможных угрозах из различных источников: файервол, антивирус, межсетевой экран и др., потом проводят анализ и могут среагировать на вероятность возникновения потенциальной угрозы, предупредив о ней заранее.

3) Брандмаузер и фаервол	c) Это специальная система шифрования вашей информации. Шифровка происходит таким образом, что для того, чтобы расшифровать нужную информацию, необходимо обладать специальным шифром.
4) Криптографическое преобразование	d) Это специализированные средства, которые контролируют выход во всемирную паутину, при необходимости фильтруют или блокируют сетевой трафик.

15. Установить соответствие средств информационной защиты:

1) Программы-антивирусы	a) Это специальные технологии, которые предотвращают потерю конфиденциальной информации. Как правило, данная технология используется большими предприятиями, так как требует больших финансовых и трудоресурсных затрат.
2) VPN	b) Борются с самыми распространенными вирусами, также способны восстанавливать поврежденные файлы.
3) DLP-решения	c) Это облачные решения для обеспечения антивирусной защиты вашего ресурса.

16. Установить соответствие степеней происхождения угрозы информационной безопасности:

1) Естественная	a) Данные угрозы, в свою очередь, делятся на 2 подкатегории: преднамеренная подкатегория — это действия хакеров, конкурентов, недобросовестных сотрудников и т. д., непреднамеренная — действия происходят из-за людей по их неосторожности.
2) Искусственная	b) Это те угрозы, которые не зависят от деятельности человека: землетрясения, ураганы, смерчи, дожди, молнии и т. д.

3) Внутренняя	c) Все угрозы, которые происходят вне системы.
4) Внешняя	d) Угроза исходит изнутри самой системы.

17. Установить соответствие каналов утечки:

1) Несанкционированное копирование, уничтожение или подделка информации	a) Ошибки персонала и пользователей
2) Перебои электропитания	b) Из-за некорректной работы программ
3) Случайное уничтожение или изменение данных	c) Потери информации, связанная с несанкционированным доступом
4) Потеря или изменение данных при ошибках по	d) Сбои оборудования, при котором теряется информация

18. Установить соответствие:

1) Программно-аппаратные (технические) методы	a) Для обеспечения безопасности используются приемы «перестраховки», с помощью которых исключается возможность ошибочного или несанкционированного проникновения в информационную систему
2) Физическая защита	b) Для осуществления информационной защиты используются специальные компьютерные технологии. С их помощью можно скрыть важные данные, не допустить утечки во время пересылки через интернет
3) Морально-этические методы	c) Профилактические действия, в основном, воспитательного характера
4) Технологические приемы	d) Мероприятия направлены на снижение риска потери данных и выявление лиц, пытающихся проникнуть на охраняемую территорию или в информационную систему

19. Установить соответствие:

1) Рабочая станция	a) Специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами
2) Сервер	b) Согласованный набор стандартных это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
3) Сетевая технология	c) Это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
4) Информационно-коммуникационная технология	d) Это информационная технология работы в сети, позволяющая людям общаться, оперативно получать информацию и обмениваться ею

20. Установить соответствие:

1) Канал связи	a) Это путь для передачи данных от одной системы к другой
2) Логический канал	b) Путь или средство, по которому передаются сигналы
3) Трафик	c) Это поток сообщений в сети передачи данных

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. На вход алгоритма хеширования SHA-1 подается сообщение длиной 2590 битов. Сколько битов будет содержать дополнение сообщения?

2. В SHA-512 покажите значение поля длины в шестнадцатеричной форме для длины сообщения 10000000 битов.

3. Каково дополнение для SHA-512, если длина сообщения 5120 битов?

4. Какое минимальное и максимальное число битов дополнения можно добавить к сообщению?

5. На вход алгоритма хеширования SHA-1 подается сообщение длиной 6143 битов. Сколько битов будет содержать дополнение сообщения?

6. В SHA-512 покажите значение поля длины в шестнадцатеричной форме для длины сообщения 100000 битов.

7. Сколько символов потребуется для записи биткоин-адреса в кодировке Base58Check?

8. Если 0 - точка в бесконечности и имеются две точки P и Q, имеющие координаты вида P (a, b) и Q (a, -b), тогда чему будет равно сложение на эллиптической кривой этих точек P + Q?

9. Каково дополнение для SHA-512, если длина сообщения 5121 битов?

10. На вход алгоритма хеширования SHA-1 подается сообщение длиной 5120 битов. Сколько битов будет содержать дополнение сообщения?

11. Каково дополнение для SHA-512, если длина сообщения 6143 битов?

12. Сколько байт в двоичной записи биткоин-адреса в кодировке Base58Check составляет контрольная сумма?

13. В SHA-512 покажите значение поля длины в шестнадцатеричной форме для длины сообщения 1000 битов.

14. На вход алгоритма хеширования SHA-1 подается сообщение длиной 5121 битов. Сколько битов будет содержать дополнение сообщения?

15. Найдите результат функции f_{47} (B, C, D), если

B = 1234 5678 ABCD 2345 34564 5678 ABCD 2468

C = 2234 5678 ABCD 2345 34564 5678 ABCD 2468

D = 3234 5678 ABCD 2345 34564 5678 ABCD 2468

16. Каково дополнение для SHA-512, если длина сообщения 6143 битов?

17. В SHA-512 покажите значение поля длины в шестнадцатеричной форме для длины сообщения 10000000 битов.

18. На вход алгоритма хеширования SHA-1 подается сообщение длиной 5120 битов. Сколько битов будет содержать дополнение сообщения?

19. Сколько символов включает алфавит кодировки Base58?

20. В SHA-512 покажите значение поля длины в шестнадцатеричной форме для длины сообщения 10000 битов.

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.