МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *29* » *августа* 2023 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 – 2023

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

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.
9. Что подразумевается под технологией распределенных реестров и какие основные принципы лежат в её основе?
10. Какие характеристики и преимущества имеет технология распределенных реестров по сравнению с традиционными централизованными системами?

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.
6. Что такое структура связи в распределенных системах и как она обеспечивает взаимодействие между узлами?
7. Какие основные типы структур связи в распределенных системах можно выделить?
8. Какая роль узлов и каналов связи в структуре распределенных систем?
9. Каким образом устанавливается связь между узлами в распределенных системах?
10. Какие преимущества и недостатки имеют различные структуры связи в распределенных системах?

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.
7. Какие основные типы операционных систем используются в настоящее время?
8. Какие функции и возможности предоставляют современные операционные системы для пользователей?
9. Какие технологии и концепции входят в современные операционные системы для обеспечения безопасности данных и защиты от вредоносных программ?
10. Какие тренды и инновации можно наблюдать в развитии операционных систем в последнее время?

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.
8. Что такое распределенная файловая система и какие преимущества она предоставляет?
9. Какие основные принципы обеспечивают надежность и отказоустойчивость в распределенных файловых системах?
10. Какие распределенные файловые системы наиболее популярны на сегодняшний день и в чем их отличие?

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.
9. Какие основные меры обеспечивают безопасность в блокчейн-технологии?
10. Какие уязвимости могут возникнуть в блокчейн-сетях и как они могут быть предотвращены?

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 ПРОИЗВОДСТВЕННЫЕ ЗАДАЧИ

1. Задача по внедрению технологии блокчейн в сферу поставок: Ваша компания занимается оптимизацией цепочки поставок для крупного производителя. Вам поручено провести исследование и реализовать систему на базе технологии блокчейн для обеспечения прозрачности и отслеживаемости поставок, уменьшения рисков и повышения эффективности процесса.

2. Задача по созданию платформы для обмена цифровыми активами: Ваша компания планирует разработать платформу, которая позволит пользователям обмениваться различными цифровыми активами, такими как криптовалюты, токены и др. Ваша задача состоит в разработке архитектуры платформы, выборе подходящей технологии распределенных реестров и реализации безопасных механизмов обмена активами.

3. Задача по созданию системы голосования на базе распределенного реестра: Ваша компания получила заказ на разработку системы голосования, которая обеспечит прозрачность и надежность процесса голосования. Вам необходимо выбрать подходящую технологию распределенных реестров, разработать систему, обеспечить безопасность данных и гарантировать конфиденциальность голосов.

4. Задача по обеспечению безопасности финансовых транзакций: Ваша компания специализируется на финансовых технологиях, и вам поручено создать систему для обеспечения безопасности финансовых транзакций. Ваша задача - выбрать подходящую технологию распределенных реестров, разработать систему, которая обеспечит конфиденциальность, целостность и аутентификацию транзакций.

5. Разработка и реализация системы учета товаров на базе технологии распределенных реестров: Ваша задача состоит в создании системы учета товаров, используя технологию распределенных реестров. Система должна обеспечивать прозрачность и надежность записей о перемещении товаров от производителя до конечного потребителя. Вам нужно разработать и внедрить алгоритмы проверки подлинности и целостности записей, а также обеспечить возможность отслеживания истории перемещений товаров.

6. Создание платформы для безопасного обмена медицинскими данными: Ваша компания получила задание разработать платформу для безопасного обмена медицинскими данными между различными медицинскими учреждениями. Используя технологию распределенных реестров, вам нужно создать систему, которая обеспечит безопасность, конфиденциальность и непрерывность обмена медицинскими данными. Задача также включает разработку механизмов авторизации и аутентификации участников платформы.

7. Разработка системы голосования на базе технологии блокчейн: Вам поручено создать систему голосования, которая обеспечит прозрачность, надежность и защиту от подделки голосов. Используя технологию блокчейн, вам нужно разработать алгоритмы для регистрации голосов, формирования блоков с голосами и проверки подлинности голосования. Задача также включает создание интерфейса для участников голосования и обеспечение безопасности системы.

8. Задача по созданию прототипа системы на базе DLT: Ваша команда разработчиков должна создать прототип системы, использующей технологии распределенных реестров. Задача включает определение требований к системе, проектирование архитектуры, разработку и тестирование прототипа. Прототип должен демонстрировать основные функциональности и преимущества, которые может предложить DLT.

9. Задача по внедрению системы DLT в организацию: Вашей организации требуется внедрить технологию распределенных реестров для оптимизации и обеспечения безопасности бизнес-процессов. Ваша задача состоит в разработке и реализации плана внедрения системы DLT. Это включает определение сфер применения, выбор конкретной технологии DLT, обучение сотрудников и переход на новую систему.

10. Задача по обеспечению безопасности системы DLT: Ваша задача - разработать и реализовать меры безопасности для системы, использующей технологию распределенных реестров. Это включает защиту от несанкционированного доступа, обеспечение целостности данных, шифрование информации и другие меры. Вам также может потребоваться проведение аудита безопасности и обучение сотрудников по вопросам информационной безопасности.

Критерии оценки:

7-12 баллов 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.

1-6 баллов 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.

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ К ЛАБОРАТОРНЫМ РАБОТАМ

Контрольные вопросы лабораторной работе №1.

1. Что такое хэширование и как оно связано с блокчейн-технологией?
2. Какие алгоритмы хеширования широко применяются в построении блокчейн-цепочки?
3. Какие данные обычно подвергаются хешированию в блокчейн?
4. Какова роль хеш-функций в формировании блоков и цепочки блоков?
5. Какие свойства у хеш-функций должны быть удовлетворены для безопасного функционирования блокчейна?
6. В чем состоит процесс формирования блокчейн-цепочки с использованием хеш-функций?
7. Какое значение имеет хеш предыдущего блока при создании нового блока?
8. Как обеспечивается непротиворечивость и целостность блокчейн-цепочки?
9. Что происходит, если изменить данные в одном из блоков цепочки?
10. Как модуль хеширования обеспечивает безопасность и доверие в блокчейн-сети?

Контрольные вопросы лабораторной работе №2.

1. Что такое проверка корректности блоков в контексте блокчейн-технологии?
2. Какие данные и хеш-функции должны быть проверены для подтверждения корректности блока?
3. Какие аспекты проверки корректности блоков учитываются при построении модуля?
4. Каким образом гарантируется, что блоки не изменяются и не подделываются?
5. Какие проверки могут быть включены в модуль для определения недействительных блоков?
6. Какой алгоритм используется для верификации целостности данных в блоке?
7. Как проверяется правильность хеша предыдущего блока при проверке блока?
8. Как обнаруживается, если блок содержит некорректные или недействительные данные?

9. Какие последствия возникают при обнаружении недействительных блоков в блокчейн-цепочке?

10. Какие меры безопасности можно предпринять для устранения возможности подтасовки блоков в блокчейне?

Контрольные вопросы лабораторной работе №3.

1. Что такое сложность хеш-функции и как она связана с блокчейн-технологией?

2. Как определяется уровень сложности для хеш-функции в блокчейне?

3. Как изменение уровня сложности влияет на процесс формирования блоков и цепочки?

4. Какова роль сложности хеш-функции в обеспечении безопасности блокчейн-сети?

5. Как сложность хеш-функции связана с временем, необходимым для создания нового блока?

6. Какие факторы могут быть учтены при установке сложности хеш-функции?

7. Как изменение сложности может повлиять на энергопотребление и вычислительные мощности блокчейн-сети?

8. Какое значение имеет сложность хеш-функции при согласовании блокчейн-цепочки в сети?

9. Какой алгоритм используется для определения сложности хеш-функции в блокчейне?

10. Какие преимущества и недостатки связаны с разными уровнями сложности хеш-функции в блокчейне?

Контрольные вопросы лабораторной работе №4.

1. Что такое проверка целостности блокчейн-цепочки и почему она важна?

2. Какие данные и хеш-функции используются для проверки целостности блока в цепочке?

3. Какие аспекты проверки целостности учитываются при построении модуля?

4. Как проверяется правильность хеша предыдущего блока при проверке целостности всей цепочки?

5. Какие меры предпринимаются для обнаружения и обработки неправильных или потерянных блоков?

6. Как обеспечивается невозможность удаления или изменения блоков из цепочки?

7. Как модуль проверки целостности блокчейн-цепочки связан с модулем проверки корректности блоков?

8. Что происходит, если были обнаружены ошибки или нарушения целостности в блокчейн-цепочке?

9. Какие меры безопасности могут быть применены для защиты от атак на целостность блокчейн-цепочки?

10. Какая роль играет проверка целостности в обеспечении надежности и доверия к блокчейн-сети?

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.

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.