

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

**Кафедра информационной безопасности
Факультета информационных технологий и анализа больших данных**

УТВЕРЖДАЮ

Проректор по учебной и
методической работе
_____ Е.А. Каменева

« 05 » марта 2024 г.

Валеев М.В.

Криптография и распределенные реестры

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
01.03.02 Прикладная математика и информатика,
образовательная программа
«Прикладная математика и информатика»
(Анализ данных и принятие решений в экономике и финансах)

*Рекомендовано Ученым советом Факультета
информационных технологий и анализа больших данных
(протокол от « 27 » февраля 2024 г. № 41)*

*Одобрено Кафедрой информационной безопасности
(протокол от « 06 » февраля 2024 г. № 2)*

Москва 2024

СОДЕРЖАНИЕ

1. Наименование дисциплины.....	3
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
3. Место дисциплины в структуре образовательной программы	5
4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	5
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий.....	6
5.1 Содержание тем дисциплины	6
5.2 Учебно-тематический план	7
5.3 Содержание семинаров, практических занятий.....	8
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....	9
6.1 Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	9
6.2 Перечень вопросов, заданий, тем для подготовки к текущему контролю	9
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по данной дисциплине	11
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	19
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	20
10. Методические указания для обучающихся по освоению дисциплины.....	21
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем.....	22
11.1. Комплект лицензионного программного обеспечения	22
11.2. Современные профессиональные базы данных и информационные справочные системы	22
11.3. Сертифицированные программные и аппаратные средства защиты информации	22
12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.....	22

1. Наименование дисциплины

«Криптография и распределенные реестры»

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Таблица 1

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ОПК-2	Способен использовать и адаптировать существующие математические методы и системы программирования для разработки и реализации алгоритмов решения прикладных задач	1. Системно подходит к выбору математических методов и систем программирования для решения прикладных задач. 2. Разрабатывает алгоритмы решения прикладных задач с использованием математических методов. 3. Реализует алгоритмы с использованием современных систем программирования.	Знать методы создания математического обеспечения для работы с распределенными реестрами. Уметь выбрать платформу для работы с распределенными реестрами в зависимости от решаемой задачи. Знать назначение и функционал типовых модулей корпоративных информационных систем, основные методы разработки приложений на их платформе. Уметь выбрать безопасные среды для разработки алгоритмов, протоколов и схем для решения поставленной задачи. Знать методологию разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем. Уметь выбирать платформу для работы с распределенными реестрами в зависимости

			от решаемой задачи и вести разработку программного обеспечения с использованием современных систем программирования.
ПКП-1	Способность анализировать финансовую информацию, рассчитывать финансовые показатели, в том числе, в условиях неопределенности	1. Владеет методиками расчета финансовых показателей, в том числе в условиях неопределенности. 2. Рассчитывает и интерпретирует финансовые показатели на основе финансовой информации.	Знать основы современной нормативно-правовой базы и методических документов в области информационной безопасности, защите информации, технической защите информации, включая процессы лицензирования, аттестации и сертификации, с учетом последних изменений законодательства и иных нормативно-правовых актов, связанных угрозы безопасности информации, обрабатываемой в информационных системах, построенных с использованием платформ для работы с распределенными реестрами. Уметь применять нормативно-правовые и методические документы в сфере цифровой экономики и защиты информации для обеспечения информационной безопасности систем, построенных с использованием платформ для работы с распределенными реестрами. Знать методы обработки исходных данных для последующей интерпретации финансовых показателей в автоматизированных

		3. Анализирует финансовую информацию, представленную в различной форме, с использованием современного инструментария.	финансово-банковских системах. Уметь выбрать платформу для работы с распределенными реестрами в зависимости от решаемой задачи. Знать методы анализа и обработки данных при эксплуатации автоматизированных финансово-банковских систем. Уметь визуализировать и обрабатывать данные результатов при эксплуатации автоматизированных финансово-банковских систем.
--	--	---	--

3. Место дисциплины в структуре образовательной программы

Дисциплина «Криптография и распределенные реестры» относится к Элективному циклу профиля.

4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Таблица 2

Вид учебной работы по дисциплине	Всего (в з/е и часах)	7 семестр (в часах)
Общая трудоемкость дисциплины	3 з.е., 108 ч.	108
Контактная работа - Аудиторные занятия	50	50
<i>Лекции</i>	16	16
<i>Семинары, практические занятия</i>	34	34
Самостоятельная работа	58	58
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Экзамен	Экзамен

5.Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1 Содержание тем дисциплины

Тема 1. Технология распределенных реестров

Распределенные реестры и блокчейн. Классификация распределенных реестров и блокчейна. Возможные применения. Безопасность. Масштабируемость. Трилемма блокчейна.

Блоки транзакций и их строение в пиринговой платежной системе Bitcoin. Построение цепочки блоков. Майнинг. Дерево Меркля.

Протоколы консенсуса: PoW, PoS, гибридные схемы. Возможные атаки на протоколы консенсуса. Эфириум: транзакции и блоки, виртуальная машина, полнота по Тьюрингу, смарт-контракты.

Тема 2. Математические основы теории распределенных реестров

Теория графов и сетей. Направленные и ненаправленные графы. Кольца, деревья, звезды, леса. Клики, решетки и торы. Гиперкубы. Направления.

Упорядоченные множества и решетки. Частичный и полный порядок. Представление частично упорядоченных множеств. Векторные часы. Решетки и их строение.

Вычислительная теория чисел. Простые и составные числа. Большие простые числа. Теорема Ферма. Квадратичные вычеты по простому модулю. Квадратичные вычеты по составному модулю. Тесты на простоту.

Сложность алгоритмов. Понятие вычислительной модели. Классы P и NP. Полиномиальная сводимость NP-полной задачи.

Вероятностные алгоритмы. Альтернативные криптосистемы. Квантовые вычисления. Решеточные алгоритмы. Задача нахождения кратчайшего вектора.

Тема 3. Криптографические протоколы

Современная криптография. Криптографические примитивы.

Односторонние функции. Функции хэширования. Стандарты, связанные с функциями хэширования. Псевдослучайность.

Целостность. Протоколы аутентификации и электронной подписи.

Стандарты электронной подписи.

Доказательства с нулевым разглашением. Математика схем разделения секрета. Пороговые функции.

Тема 4. Консенсус и время в распределенных системах

Децентрализованные системы. Консенсус Накамото. Анализ стойкости. Системы с разрешением.

Византийский консенсус (BFT). Теоремы о невозможности.

Логические часы. Скалярное время Лэмпорта. Векторное время. Матричное время. Проблема эффективности.

5.2 Учебно-тематический план

Таблица 3

№ п/ п	Наименование тем (разделов) дисциплины	Трудоёмкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа* Аудиторная работа			Самосто- ятельная работа	
			Общая, в т.ч.:	Лекции	Семинары, практичес- кие занятия		
1.	Технология распределенных реестров	20	10	4	6	10	Доклады, презентации и дискуссии
2.	Математические основы теории распределенных реестров	36	18	4	14	18	Доклады, презентации и дискуссии
3.	Криптографичес- кие протоколы	34	16	4	12	18	Доклады, презентации и дискуссии
4.	Консенсус и время в распределенных системах	18	6	4	2	12	Доклады, презентации и дискуссии
	В целом по дисциплине	108	50	16	34	58	Согласно учебному плану: контрольная работа
	ИТОГО в %	100	46	32	68	54	

*объем контактной работы в очно-заочной/заочной формах обучения и индивидуальных учебных планах определяется соответствующими учебными планами. Темы, реализуемые в виде контактной работы, определяются преподавателем самостоятельно, исходя из уровня их сложности.

5.3 Содержание семинаров, практических занятий

Таблица 4

№ темы	Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях, рекомендуемые источники из разделов 8, 9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
1.	Технология распределенных реестров	1. Распределенные реестры и блокчейн. Классификация распределенных реестров и блокчейн. Возможные применения. Безопасность. Масштабируемость. Источники: 8.1, 9.2, 9.17, 9.18	Доклады, групповые дискуссии, практикум по решению задач, проверочные работы.
2.	Математические основы теории распределенных реестров	1. Топология графов. Примеры графов. Перечисление графов. Подсчет числа ребер и вершин. Источники: 8.2, 8.3, 8.4 2. Свойства решеток. Полное упорядочение, согласованное с частичным порядком. Теорема Дилуорса и ее следствия. Примеры решеток. Примеры векторных часов. Источники: 8.1, 8.2, 8.3, 8.4 3,4. Алгоритмы разложения составных чисел на простые множители. Построение больших простых чисел. Освоение системы компьютерной алгебры Mathematica. Теорема Ферма. Квадратичные вычеты по простому модулю. Квадратичные вычеты по составному модулю. Тестирование чисел на простоту. Эллиптические кривые. Источники: 8.4	Доклады, групповые дискуссии, практикум по решению задач, проверочные работы.
3.	Криптографические протоколы	1. Криптография и теория сложности. Источники: 8.3. 2. Криптографические хэш-функции. Источники: 8.3. 3. Схема электронной подписи RSA. Протокол аутентификации. Источники: 8.2, 8.3 4. Схемы электронной подписи. Источники: 8.2, 8.3, 9.13, 9.14, 9.15 5. Тесты простоты Источники: 8.3. 6. Схемы разделения секрета Источники: 8.3.	Групповая дискуссия, практикум по решению задач, проверочная работа.

4.	Консенсус и время в распределенных системах	1. Сравнительный анализ схем консенсуса по Накамото и BFT. Источники: 9.17, 9.22, 9.25	Групповая дискуссия, практикум по решению задач, проверочная работа.
----	---	---	--

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1 Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Таблица 5

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Технология распределенных реестров	Изучение проектов внедрения технологий распределенных реестров в финансовой сфере.	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций
Математические основы теории распределенных реестров	Классы сложности алгоритмов. Классы функций хэширования. Различные подходы к представлению упорядоченных множеств. Процессы в распределенных системах.	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций
Криптографические протоколы	Безопасность криптографических протоколов, утвержденных стандартами. Сравнение отечественных и зарубежных стандартов.	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций
Консенсус и время в распределенных системах	Сравнительный анализ схем консенсуса.	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций

6.2 Перечень вопросов, заданий, тем для подготовки к текущему контролю

Примерные вопросы тем докладов с презентациями и дискуссий

1. Каковы основные принципы криптографии?
2. Какие типы алгоритмов шифрования существуют?
3. Каким образом работает алгоритм RSA?
4. Какие возможности криптографии для защиты данных в современном мире?

5. Что такое распределенный реестр (блокчейн) и как он используется?
6. Какие преимущества распределенных реестров перед централизованными базами данных?
7. Каким образом осуществляется проверка транзакций в блокчейне?
8. Какие проблемы могут возникнуть при использовании блокчейна?
9. Какие криптографические методы используются для защиты блокчейна?
10. Каким образом происходит майнинг в блокчейне?
11. Какие новые технологии криптографии и блокчейна разрабатываются в настоящее время?
12. Каким образом осуществляется шифрование данных в блокчейне?
13. Какие принципы защиты конфиденциальности данных применяются в блокчейне?
14. Какие принципы децентрализации применяются в блокчейне?
15. Каким образом происходит хранение данных в блокчейне?
16. Каковы основные принципы работы криптовалют и их защиты?
17. Какие возможности предоставляют умные контракты в блокчейне?
18. Каким образом реализуется обеспечение безопасности транзакций в блокчейне?
19. Какие проблемы масштабирования и производительности возникают при использовании блокчейна?
20. Каким образом различные типы блокчейнов могут быть использованы в различных отраслях?
21. Какие технологии криптографии могут быть применены для улучшения безопасности блокчейна?
22. Каким образом криптография может изменить способы работы цифровых платежей?
23. Каким образом возможно использование криптографии и блокчейна в медицинской сфере?
24. Каким образом можно улучшить защиту данных с помощью распределенных реестров?
25. Каким образом криптография и блокчейн могут повлиять на традиционные способы хранения и передачи данных?

Примерные вопросы к контрольной работе

1. Простые и составные числа. Разложение составных чисел на простые множители.
2. Эллиптические кривые.
3. Сложение точек на эллиптической кривой.

4. Циклические подгруппы группы точек эллиптической кривой.
5. Процесс формирования электронной подписи сообщения.
6. Алгоритм проверки электронной подписи.
7. Функции хэширования.
8. Стандарты электронной подписи.

Примеры заданий контрольной работы

Заданы: простое число p ; эллиптическая кривая $E: y^2 = x^3 + ax + b$ над полем $\mathbf{F}_p$; точка $P(x, y) \in E$, порождающая циклическую подгруппу.

В качестве хэш-функции использовать функцию $f(x) = x^2 \bmod 61$, $f: \{0,1\}^* \rightarrow \{0,1\}^5$.

1. Сформировать закрытый ключ d и открытый ключ $Q = d \cdot P$ в соответствии со схемой подписи ГОСТ Р 34.10-2012 (ECDSA).

2. Сформировать подпись под сообщением длиной 2 байта и передать подписанное сообщение партнеру.

3. Получив от партнера подписанное сообщение и открытый ключ, верифицировать подпись.

Данные для составления схем подписи

Вариант	p	a	b	x	y	Порядок точки
1	83	1	8	6	8	79
2	83	5	7	30	4	101
3	79	1	6	35	16	97
4	79	10	3	26	8	83

Ключ должен быть индивидуальным для каждого участника.

Замечание. Во втором ресурсе координаты точек на эллиптической кривой указываются в шестнадцатеричном формате. Точка 0 на эллиптической кривой может быть представлена любой точкой, координаты которой не удовлетворяют уравнению кривой.

Работу нужно выполнить на листах формата А4. В работе должна быть описана схема вычислений с указанием результата на каждом шаге (подробности выполнения операций с точками эллиптических кривых приводить не требуется).

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по данной дисциплине

Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине содержится в разделе «2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Таблица 6

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ОПК-2 Способен использовать и адаптировать существующие математические методы и системы программирования для разработки и реализации алгоритмов решения прикладных задач	Индикатор 1 Системно подходит к выбору математических методов и систем программирования для решения прикладных задач.	Знать методы создания математического обеспечения для работы с распределенными реестрами. Уметь выбрать платформу для работы с распределенными реестрами в зависимости от решаемой задачи.	Задание 1. Описать алгоритм работы скалярных часов Лэмпорта в распределенной системе. Для заданной схемы, содержащий несколько процессов (нодов) и событий, включая транзакции между нодами, расставить временные отметки, используя алгоритм Лэмпорта.
	Индикатор 2 Разрабатывает алгоритмы решения прикладных задач с использованием математических методов.	Знать назначение и функционал типовых модулей корпоративных информационных систем, основные методы разработки приложений на их платформе. Уметь выбрать безопасные среды для разработки алгоритмов, протоколов и схем для решения поставленной задачи.	Задание 1. События e_i и e_j происходят в процессах P_i и P_j и им векторные временные метки VT_{e_i} и VT_{e_j} соответственно. Доказать, что в этом событие e_i предшествует событию e_j в том и только том случае, когда $VT_{e_i}[i] < VT_{e_j}[j]$. Задание 2. Составить перечень математических методов решения задач в области информационной

			безопасности систем, построенных с использованием технологии блокчейн.
	Индикатор 3 Реализует алгоритмы с использованием современных систем программирования.	Знать методологию разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем. Уметь выбирать платформу для работы с распределенными реестрами в зависимости от решаемой задачи и вести разработку программного обеспечения с использованием современных систем программирования.	Задание 1. Провести сравнительный анализ программных платформ «Биткоин» и «Эфириум» для создания сервиса по обмену жилыми помещениями. Задание 2. Предположим, что агенты A_1 и A_2 передают друг другу информацию, используя алгоритм RSA. Пусть N_i, e_i, d_i соответственно открытый модуль, открытый ключ и секретный ключ агента $A_i, i = 1, 2$. Для передачи подписанного сообщения m агенту A_2 агент A_1 поступает следующим образом. Зашифровывает свое сообщение, вычисляя $c \equiv m^{e_2} \bmod N_2$; применяя функцию хэширования, вычисляет $s \equiv Hash(m)^{d_1} \bmod N_1$ и пересылает агенту A_2 пару (c, s). Описать алгоритм извлечения агентом A_2 исходного сообщения m и верификации подписи. Оценить возможность подделки подписи злоумышленником.
ПКП-1 Способность анализировать финансовую информацию, рассчитывать	Индикатор 1 Владеет методиками расчета финансовых показателей, в том числе в условиях неопределенности.	Знать основы современной нормативно-правовой базы и методических документов в	Задание 1. Составить классификацию современной нормативно-правовой базы и методических

финансовые показатели, в том числе, в условиях неопределенности		области информационной безопасности, защите информации, технической защите информации, включая процессы лицензирования, аттестации и сертификации, с учетом последних изменений законодательства и иных нормативно-правовых актов, связанных угрозы безопасности информации, обрабатываемой в информационных системах, построенных с использованием платформ для работы с распределенными реестрами. Уметь применять нормативно-правовые и методические документы в сфере цифровой экономики и защиты информации для обеспечения информационной безопасности систем, построенных с использованием платформ для работы с распределенными реестрами.	документов в области информационной безопасности технологии блокчейн. Задание 2. События e_i и e_j происходят в процессах P_i и P_j и им векторные временные метки VT_{e_i} и VT_{e_j} соответственно. Доказать, что в этом событие e_i предшествует событию e_j в том и только том случае, когда $VT_{e_i}[i] < VT_{e_j}[j]$.
	Индикатор 2 Рассчитывает и интерпретирует финансовые показатели на основе	Знать методы обработки исходных данных для последующей интерпретации	Задание 1. Описать угрозы безопасности информации и способы их нейтрализации для информационных

	финансовой информации.	финансовых показателей в автоматизированных финансово-банковских системах. Уметь выбрать платформу для работы с распределенными реестрами в зависимости от решаемой задачи.	систем, построенных с использованием гибридного блокчейна.
	Индикатор 3 Анализирует финансовую информацию, представленную в различной форме, с использованием современного инструментария.	Знать методы анализа и обработки данных при эксплуатации автоматизированных финансово-банковских систем. Уметь визуализировать и обрабатывать данные результатов при эксплуатации автоматизированных финансово-банковских систем.	Задание 1. Предложить комплекс организационных мер, направленных на защиту информации в автоматизированных финансово-банковских системах, построенных с использованием технологии блокчейн. Задание 2. Интерпретируйте значение коэффициента оборачиваемости дебиторской задолженности.

Примерный перечень вопросов для подготовки к экзамену

1. Определение понятий блокчейна и распределенного реестра.
2. История развития технологии блокчейн и распределенных реестров.
3. Основные технологии распределённого реестра. (блокчейн, хэшграф, направленный ациклический граф). Преимущества и недостатки.
4. Структура и жизненный цикл транзакций, устройство блоков транзакций, механизм формирования цепочки блоков.
5. Протоколы сетевого взаимодействия в распределенных реестрах и блокчейн.
6. Алгоритмы консенсуса и принципы их работы.
7. Понятие смарт-контрактов и принципы их работы.

8. Проблемы масштабируемости распределенных реестров и существующие решения.
9. Примеры использования технологии распределенных реестров для решения индустриальных задач.
10. Понятие дерева Меркля.
11. Принятие решения о подтверждении нового блока.
12. Разница между Эфириум и Биткойн.
13. Понятие полноты по Тьюрингу.
14. Понятие направленного и ненаправленного графа.
15. Принципы построения компьютерных сетей. Основные топологии построения. Маршрутизация в сетях.
16. Построить продолжение частично порядка до линейного.
17. Построить транзитивное замыкание заданного бинарного отношения на конечном множестве.
18. Представить конечное упорядоченное множество в виде объединения непересекающихся цепей.
19. Вычислить значение функции Эйлера для заданного составного числа.
20. Алгоритм решения системы линейных сравнений.
21. Установить, является ли заданное число квадратичным вычетом по указанному простому модулю.
22. Используя тест на простоту, определить, является ли заданное число простым.
23. Классы P, NP, NP-Complete, NP-Hard. Примеры. Сводимость задач из разных классов.
24. Сложность задачи нахождения кратчайшего вектора решётки.
25. Сложность задачи нахождения клики графа.
26. Сложность задачи нахождения Эйлера цикла на графе из n рёбер.
27. Основные вычислительно сложные задачи криптографии на решётках.
28. Приведите примеры NP-полных задач.
29. Основные криптографические примитивы для обеспечения конфиденциальности и целостности передаваемой информации.
30. На какие вычислительные задачи опирается асимметричный алгоритм электронной подписи.
31. Понятие криптографической стойкости. Требования к криптографическим хэш-функциям.
32. Применение парадокса «дней рождения» для исследования стойкости криптографических хэш-функций.
33. Основные известные алгоритмы хэширования. Пример криптографических и не криптографических функций хэширования.

- 34.Схема Эль-Гамала. Определение и основные элементы. Предположения о стойкости. Алгоритм генерации ключей. Алгоритм подписи.
35. Протокол Диффи-Хеллмана над простым полем $\mathbb{Z}_p$. Описание алгоритма. Предположения о стойкости. Пример для заданных значений.
- 36.Схема RSA. Определение и основные элементы. Предположения о стойкости. Алгоритм создания и проверки электронной подписи. Пример для заданных значений.
- 37.Алгоритм сложения заданных точек указанной эллиптической кривой.
- 38.Провести расчеты по протоколу электронной подписи, основанному на эллиптических кривых.
- 39.Доказательство с нулевым разглашением. «Пещера нулевого разглашения». Отличия ZK-STARK и ZK-SNARK.
- 40.Схемы разделения секрета. Основные примеры построения. Утверждения о стойкости.
- 41.Для заданной распределенной системы, содержащий несколько процессов (нодов) и событий, включая транзакции между нодами, расставить временные отметки, используя алгоритм Лэмпорта
- 42.Консенсус Накамото. Определение и основные сферы применения.
- 43.Протоколы консенсуса (PoW, PoS, PoA, DPoS, и др.) Преимущества и недостатки.
- 44.Задача Византийских генералов. Византийский консенсус (BFT).
- 45.Сформулировать теоремы о невозможности.
- 46.Скалярное время Лампорта.
- 47.Векторное время и матричное время.

Пример экзаменационного билета

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

Департамент Информационной безопасности

Дисциплина «Криптография и распределенные реестры»

Факультет информационных технологий и анализа больших данных

Форма обучения очная

Семестр 7

Направление 01.03.02 «Прикладная математика и информатика»

ОП «Прикладная информатика и информатика» (Анализ данных и принятие решений в экономике и финансах)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Структура и жизненный цикл транзакций, устройство блоков транзакций, механизм формирования цепочки блоков (10 баллов).
2. Схема Эль-Гамала. На чём основана. Алгоритм генерации ключей. Алгоритм подписи. (20 баллов).
3. В криптосистеме RSA при модуле 437 и открытом ключе 117 определите закрытый ключ и подпись сообщения 303 (30 баллов).

Подготовил _____ (Валеев М.В.)

На основе перечня теоретических вопросов и практико-ориентированных заданий,
утвержденного на заседании Департамента информационной безопасности (протокол № ____
от _____)

Утверждаю: руководитель департамента _____ А.В. Царегородцев

Дата _____

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

Рекомендуемая литература

а) основная:

1. Бабичев, С. Л. Распределенные системы: учебное пособие / С. Л. Бабичев, К. А. Коньков. – Москва : Юрайт, 2023. – 507 с. – ЭБС Юрайт. – URL: <https://www.biblio-online.ru/bcode/518274> (дата обращения: 13.12.2023). – Текст : электронный.

2. Гисин, В. Б. Дискретная математика : учебник и практикум для вузов / В. Б. Гисин ; Финуниверситет. — Москва : Юрайт, 2016 .— 383 с. — Текст непосредственный. — То же. — 2023. — 383 с. — ЭБС Юрайт. — URL: <https://urait.ru/bcode/510972> (дата обращения: 13.12.2023). — Текст : электронный.

3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Юрайт, 2023. — 209 с. — (Высшее образование). — ЭБС Юрайт. — URL: <https://urait.ru/bcode/511700> (дата обращения: 13.12.2023). — Текст : электронный.

4. Hoffstein, J. An introduction to mathematical cryptography / J. Hoffstein, J. Pipher, J. H. Silverman, & J. H. Silverman. – New York : Springer, 2014 (2nd edition). – 538 p. — 2018. — ЭБС Springer Link. — URL: <https://link.springer.com/book/10.1007/978-1-4939-1711-2> (дата обращения 13.12.2023). — Текст : электронный.

б) дополнительная:

5. Романьков, В. А. Введение в криптографию : курс лекций / В. А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2023. – 240 с. – (Высшее образование: Бакалавриат). - ЭБС ZNANIUM.com. - URL: <https://znanium.com/catalog/product/1937958> (дата обращения: 13.12.2023). - Текст : электронный.

6. Rubinstein-Salzedo S. Cryptography / S. Rubinstein-Salzedo. – Springer, 2018. — 260 p. — ЭБС Springer Link. — URL: <https://link.springer.com/book/10.1007/978-3-319-94818-8> (дата обращения 13.12.2023). — Текст : электронный.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Сайт Центрального банка Российской Федерации: www.cbr.ru
2. Дорожная карта развития «сквозной» цифровой технологии «системы распределенного реестра». Режим доступа: https://digital.gov.ru/uploaded/files/07102019srr.pdf?utm_referrer=https%3a%2f%2fwww.google.com%2f
3. Сайт Федерального агентства по техническому регулированию и метрологии: www.gost.ru.
4. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/> (<http://library.fa.ru/files/elibfa.pdf>)
5. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
6. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
7. Электронно-библиотечная система Znaniium <http://www.znaniium.com>
8. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
9. Электронно-библиотечная система издательства Проспект <http://ebs.prospekt.org/books>
10. Электронно-библиотечная система издательства Лань <https://e.lanbook.com/>
11. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
12. Информационно-образовательный портал Финансового университета при Правительстве Российской Федерации <http://portal.ufrf.ru/>
13. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» <https://www.altell.ru/legislation/standards/gost-34.10-2012.pdf>
14. ГОСТ Р 34.10-2018 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи <https://protect.gost.ru/document.aspx?control=7&id=232149>
15. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования. <https://meganorm.ru/Data2/1/4293788/4293788459.pdf>
16. МР 26.4.001-2018 «Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров». Режим доступа: <https://tc26.ru/standarts/metodicheskie-rekomendatsii/mr-26-4-001-2018-terminy-i->

opredeleniya-v-oblasti-tehnologiy-tsepnoy-zapisi-dannykh-blokcheyn-i-raspredelennykh-reestrov.html

17. Развитие технологии распределенных реестров. М: ЦБР, 2017, 1-16. https://www.cbr.ru/content/document/file/36007/reestr_survey.pdf

18. Технология распределенного реестра: за рамками блокчейн. — Правительство. Управление науки. Отчет главного научного советника Правительства Великобритании, 2015. — с. 1-88. <https://mpdblog.ru/wp-content/uploads/2017/07/bitcoin-tehnologia-raspredelennogo.pdf>

19. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>

20. Калькулятор для вычислений с эллиптическими кривыми <http://extranet.cryptomathic.com/ecc/index>

21. Система компьютерной алгебры Maxima <http://maxima.sourceforge.net/ru/>

22. Baird L. The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance //Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep. – 2016. — Режим доступа: <http://pages.cpsc.ucalgary.ca/~joel.reardon/blockchain/readings/hashgraph.pdf>

23. Buterin V. A next-generation smart contract and decentralized application platform. White paper. — Режим доступа: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

24. Buterin V. Ethereum white paper. GitHub repository. — Режим доступа: <https://github.com/ethereum/wiki/wiki/White-Paper>

25. Nakamoto S. et al. Bitcoin: A peer-to-peer electronic cash system. – 2008. — Режим доступа: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.221.9986&rep=rep1&type=pdf>

26. Ethereum: a secure decentralised generalised transaction ledger – 2022-10-24. Режим доступа: <https://ethereum.github.io/yellowpaper/paper.pdf>

10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов реализуется в соответствии с приказом Финансового университета от 11.05.2021 № 1040/о «Об утверждении Методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете». Промежуточная аттестация проводится в соответствии с приказом Финансового университета от

23.03.2017 № 0557/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры в Финансовом университете». Департаментом могут разрабатываться дополнительные методические рекомендации для отдельных форм проведения аудиторных занятий и самостоятельной работы студентов.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

11.1. Комплект лицензионного программного обеспечения

Windows, Microsoft Office;
Антивирус Kaspersky

11.2 Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Консультант Плюс»
2. Информационно-правовая система «Гарант»
3. Электронная энциклопедия: <http://ru.wikipedia.org/wiki/Wiki>
4. Система комплексного раскрытия информации «СКРИН»

11.3. Сертифицированные программные и аппаратные средства защиты информации

Не предусмотрены.

12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Занятия по дисциплине проводятся в аудиториях, оборудованных мультимедийными комплексами, компьютерами с выходом в Интернет.