


**Федеральное государственное образовательное бюджетное
учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)
Департамент анализа данных, принятия решений и
финансовых технологий**

УТВЕРЖДАЮ

Проректор по развитию
образовательных программ


Каменева Е.А.
«22» октября 2019 г.

Гисин В.Б.

КРИПТОГРАФИЯ И РАСПРЕДЕЛЕННЫЕ РЕЕСТРЫ

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
09.03.03 «Прикладная информатика»,
профиль «ИТ-сервисы и технологии обработки данных в экономике и
финансах»

*Рекомендовано Ученым советом
факультета прикладной математики и информационных технологий
(протокол № 18 от 15.10.2019 г.)*

*Одобрено Советом учебно-научного департамента анализа данных,
принятия решений и финансовых технологий
(протокол № 3 от 15.10.2019 г.)*

Москва 2019

**Федеральное государственное образовательное
бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ
ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

**Департамент анализа данных,
принятия решений и финансовых технологий**

Гисин В.Б.

КРИПТОГРАФИЯ И РАСПРЕДЕЛЕННЫЕ РЕЕСТРЫ

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
09.03.03 «Прикладная информатика»,
профиль «ИТ-сервисы и технологии обработки данных в экономике и
финансах»

Москва 2019

**Федеральное государственное образовательное бюджетное
учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

**Департамент анализа данных, принятия решений и
финансовых технологий**

УТВЕРЖДАЮ

Проректор по развитию
образовательных программ

_____ Каменева Е.А.

«22» октября 2019 г.

Гисин В.Б.

КРИПТОГРАФИЯ И РАСПРЕДЕЛЕННЫЕ РЕЕСТРЫ

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки
09.03.03 «Прикладная информатика»,
профиль «ИТ-сервисы и технологии обработки данных в экономике и
финансах»

*Рекомендовано Ученым советом
факультета прикладной математики и информационных технологий
(протокол № 18 от 15.10.2019 г.)*

*Одобрено Советом учебно-научного департамента анализа данных,
принятия решений и финансовых технологий
(протокол № 3 от 15.10.2019 г.)*

Москва 2019

Рецензенты: А.В. Чечкин, д.ф.-м.н., профессор департамента анализа данных, принятия решений и финансовых технологий

Гисин В.Б. «Криптография и распределенные реестры». Рабочая программа дисциплины для студентов, обучающихся по направлению подготовки 09.03.03 «Прикладная информатика» профиль «ИТ-сервисы и технологии обработки данных в экономике и финансах» (программа подготовки бакалавра) — М.: Финансовый университет при Правительстве Российской Федерации, департамент «Анализ данных, принятия решений и финансовых технологий», 2019.- 18 с.

Дисциплина «Криптография и распределенные реестры» относится к Модулю дисциплин по выбору, углубляющих освоение профиля «ИТ-сервисы и технологии обработки данных в экономике и финансах», направление подготовки 09.03.03 «Прикладная информатика».

В рабочей программе дисциплины представлены цели и задачи дисциплины, требования к результатам освоения дисциплины, содержание дисциплины, тематика практических занятий и технология их проведения, формы самостоятельной работы студентов, система оценивания, учебно-методическое и информационное обеспечение дисциплины.

УДК 003.26.09

ББК _____

Учебное издание
Гисин Владимир Борисович
Криптография и распределенные реестры
Рабочая программа дисциплины

Компьютерный набор, верстка

В.Б. Гисин

Формат 60х90/16. Гарнитура Times New Roman
Усл. п.л. _____ . Изд. № _____ . Тираж - _____ экз.
Заказ № _____
Отпечатано в Финуниверситете

© В.Б. Гисин, 2019

© Финансовый университет, 2019

ОГЛАВЛЕНИЕ

1. Наименование дисциплины	4
2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	4
3. Место дисциплины в структуре образовательной программы	4
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	5
5.1. Содержание дисциплины	5
5.2. Учебно-тематический план.....	7
5.3. Содержание семинаров, практических занятий	7
6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	12
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	13
8. Методические указания для обучающихся по освоению дисциплины	14
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	15
10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	15

1. Наименование дисциплины

Криптография и распределенные реестры

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

Дисциплина «Криптография и распределенные реестры» обеспечивает формирование следующих компетенций: ПК-23, ПКП-4.

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции ¹	Результаты обучения (владения ² , умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПК-23	Способность применять системный подход и математические методы в формализации решения прикладных задач	-	Знать: основные факты теории чисел, применяемые в современной криптографии открытого ключа. Уметь: анализировать эффективность работы криптографического алгоритма, основанного на теоретико-числовых вычислениях. Владеть: навыками выбора безопасного криптографического протокола для решения поставленной задачи.
ПКП-4	Способность применять технологии моделирования и анализа процессов в сфере экономики и финансов	-	Знать: основные характеристики платформ для работы с распределенными реестрами. Уметь: выбрать платформу для работы с распределенными реестрами в зависимости от решаемой задачи. Владеть: методами создания математического обеспечения для работы с распределенными реестрами

¹ Заполняется при реализации актуализированных ОС ВО ФУ и ФГОС ВО3++

² Владения формулируются только при реализации ОС ВО ФУ первого поколения и ФГОС ВО 3+

3. Место дисциплины в структуре образовательных программ

Дисциплина «Криптография и распределенные реестры» относится к Модулю дисциплин по выбору, углубляющих освоение профиля «ИТ-сервисы и технологии обработки данных в экономике и финансах» профиль 09.03.03 «Прикладная информатика».

Дисциплина «Криптография и распределенные реестры» базируется на знаниях, полученных при изучении дисциплин «Математика», «Дискретная математика», «Анализ данных».

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

Общая трудоёмкость дисциплины составляет 3 зачётных единицы.

Вид промежуточной аттестации – зачет.

Вид текущего контроля – контрольная работа.

Очная форма обучения 2018 г.

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 5 (в часах)
Общая трудоемкость дисциплины	3 з/е, 108 ч.	108
Контактная работа - Аудиторные занятия	34	34
<i>Лекции</i>	<i>16</i>	<i>16</i>
<i>Семинары, практические занятия</i>	<i>18</i>	<i>18</i>
Самостоятельная работа	74	74
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Зачет	Зачет

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

5.1 Содержание дисциплины

1. Технология распределенных реестров

Распределенные реестры и блокчейн. Классификация распределенных реестров и

блокчейн. Возможные применения. Безопасность. Масштабируемость.

Цепочка блоков в биткоин. Транзакции и блоки. Строение блоков. PoW. Майнинг. Дерево Меркле. Протокол консенсуса. Возможные атаки. Эфириум. Транзакции и блоки. Виртуальная машина. Полнота по Тьюрингу. Смарт- контракты.

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 примарности.

Сложность алгоритмов. Понятие вычислительной модели. Классы P и NP. Полиномиальная сводимость NP-полные задачи. Вероятностные алгоритмы. Альтернативные криптосистемы. Квантовые вычисления. Решеточные алгоритмы. Проблема кратчайшего вектора.

3. Криптографические протоколы

Методы современной криптографии. Криптографические примитивы. Односторонние функции. Функции хеширования. Стандарты, связанные с функциями хеширования. Псевдослучайность. Доказательства с нулевым разглашением.

Схемы кодирования. Электронная подпись и аутентификация. Стандарты электронной подписи.

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 Лампорта. Векторное время. Матричное время. Проблема эффективности.

5.2 Учебно-тематический план

№ п/п	Наименование тем (разделов) дисциплины	Трудоёмкость в часах						Формы текущего контроля успеваемости
		Все го	Аудиторная работа				Самос тоятел ьная работа	
			Общ ая, в т.ч.:	Лекц ии	Семина ры, практич еские занятия	Занятия в интеракти вных формах		
1.	Технология распределенных реестров	20	6	4	2	2	14	Самостоятель ные работы. Участие в решении задач на практических занятиях. Собеседования по домашним заданиям.
2.	Математические основы теории распределенных реестров	36	12	4	8	6	24	
3.	Криптографические протоколы	34	10	4	6	4	24	
4.	Консенсус и время в распределенных системах	18	6	4	2	2	12	
	В целом по дисциплине	108	34	16	18	14	74	Контрольная работа.
	Итого в %					41		

5.3 Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 6,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
Технология распределенных реестров	<p>1. Распределенные реестры и блокчейн. Классификация распределенных реестров и блокчейн. Возможные применения. Безопасность. Масштабируемость.</p> <p><i>Рекомендуемые источники: п.6.[1]; п.7. [17], [16]</i></p>	Интерактивн ая форма, Практикум по решению задач по тематике занятия в малых группах (2-4 студента) и коллективное обсуждение решений
Математические основы теории распределенных реестров	<p>2. Топология графов. Примеры графов. Перечисление графов. Подсчет числа ребер и вершин. <i>Рекомендуемые источники: 6.[2], [4]</i></p> <p>3. Свойства решеток. Полное упорядочение, согласованное с частичным порядком. Теорема Дилуорта и ее следствия. Примеры решеток. Примеры векторных часов. <i>Рекомендуемые источники: 6.[1], [2], [4]</i></p> <p>4,5. Алгоритмы разложения составных чисел на простые множители. Построение больших простых чисел. Освоение системы компьютерной алгебры Maxima. Теорема Ферма. Квадратичные вычеты по простому модулю. Квадратичные вычеты по составному модулю. Тестирование чисел на простоту.</p>	Интерактивн ая форма, Практикум по решению задач по тематике занятия в малых группах (2-4 студента) и коллективное обсуждение решений

Криптографические протоколы	<p>6. Схема кодирования RSA. Протокол аутентификации. <i>Рекомендуемые источники:</i> 6. [2], [3]; 7.[4], [5]</p> <p>7. Протоколы электронно-цифровой подписи. <i>Рекомендуемые источники:</i> 6.[2], [3]; 7.[4], [5]</p> <p>8. Оценка эффективности и стойкости схем кодирования и протоколов. <i>Рекомендуемые источники:</i> 6. [3]; 7. [4], [5]</p>	Интерактивн ая форма, Практикум по решению задач по тематике занятия в малых группах (2-4 студента) и коллективное обсуждение решений
Консенсус и время в распределенных системах	<p>7. Сравнительный анализ схем консенсуса по Накамото и BFT. <i>Рекомендуемые источники:</i> 7. [17], [17], [22]</p>	Интерактивн ая форма, Практикум по решению задач по тематике занятия в малых группах (2-4 студента) и коллективное обсуждение решений

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

а) основная:

1. Бабичев, С. Л. Распределенные системы : учебное пособие для вузов / С. Л. Бабичев, К. А. Коньков. — Москва : Юрайт, 2019. — 507 с. — (Высшее образование). — ЭБС Юрайт. — URL: <https://biblio-online.ru/bcode/445188> (дата обращения: 21.01.2020). — Текст : электронный
2. Гисин, В. Б. Дискретная математика : Учебник и практикум для академического бакалавриата / В.Б. Гисин ; Финуниверситет .— М. : Юрайт, 2016 .— 383 с. — Текст непосредственный. — То же. — 2019. — 383 с. — ЭБС Юрайт. — URL: <https://biblio-online.ru/bcode/432144> (дата обращения: 21.01.2020). — Текст : электронный
3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Юрайт, 2017. — 209 с. — Текст непосредственный. — То же. — 2019 . — ЭБС Юрайт. — URL: <https://biblio-online.ru/bcode/433420> (дата обращения: 21.01.2020). — 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 21.01.2020) — Текст : электронный

б) дополнительная:

1. Романьков В.А. Введение в криптографию: курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2018. — 240 с. — ЭБС ZNANIUM — URL: <http://new.znanium.com/catalog/product/924700> (дата обращения 21.01.2020) .— Текст : электронный

2. Rubinstein-Salzedo S. Cryptography / S. Rubinstein-Salzedo . – Springer, 2018. — 260 p.— ЭБС SpringerLink.— URL: <https://link.springer.com/book/10.1007/978-3-319-94818-8> (дата обращения 21.01.2020). —Текст : электронный

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

1. Информационно-образовательный портал Финансового университета при Правительстве Российской Федерации <http://portal.ufrf.ru/>
2. Сайт департамента анализа данных, принятия решений и финансовых технологий.
3. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/> (<http://library.fa.ru/files/elibfa.pdf>)
4. ГОСТ Р 34.10-2012. *Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»* <http://www.altell.ru/legislation/standards/gost-34.10-2012.pdf>
5. ГОСТ Р 34.10-2001 *Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи* http://kaf403.rloc.ru/POVS/Crypto/GOST_R_34.10-2001.pdf
6. ГОСТ Р 34.11-2012 *Информационная технология. Криптографическая защита информации.* Функция хэширования
http://kaf403.rloc.ru/POVS/Crypto/GOST_R_34.10-2001.pdf
7. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/> (<http://library.fa.ru/files/elibfa.pdf>)
8. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
9. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
10. Электронно-библиотечная система Znanium <http://www.znaniy.com>
11. «Деловая онлайн библиотека» издательства «Альпина Паблишер» <http://lib.alpinadigital.ru/en/library>

12. Электронно-библиотечная система издательства «Лань»
<https://e.lanbook.com/>
13. Электронно-библиотечная система издательства «ЮРАЙТ»
<https://www.biblio-online.ru/>
14. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
15. Калькулятор для вычислений с эллиптическими кривыми
<http://extranet.cryptomathic.com/ecc/index>
16. Система компьютерной алгебры Maxima
<http://maxima.sourceforge.net/ru/>
17. Развитие технологии распределенных реестров. М: ЦБР, 2017, 1-16 Режим доступа: 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. — Режим доступа: <https://mpdblog.ru/wp-content/uploads/2017/07/bitkoin-tekhnologiya-raspredelennogo.pdf>
19. 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>
20. Buterin V. A next-generation smart contract and decentralized application platform. White paper. — Режим доступа:
https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf
21. Buterin V. Ethereum white paper. GitHub repository. — Режим доступа:
<https://github.com/ethereum/wiki/wiki/White-Paper>
22. Nakamoto S. et al. Bitcoin: A peer-to-peer electronic cash system. – 2008. — Режим доступа:
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.221.9986&rep=rep1&type=pdf>

8.Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов проходит аудиторно и внеаудиторно. Организации самостоятельной работы служит учебно-тематический план

изучения дисциплины. В этом плане указана тематика лекций, практических занятий, вопросы и задания для самостоятельного изучения.

Домашние задания следует выполнять регулярно при подготовке к практическим занятиям. Контроль выполнения домашних заданий осуществляется в ходе практических занятий в процессе выборочного собеседования.

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

Комплект лицензионного программного обеспечения:

Windows, Microsoft Office;

Антивирус ESET Endpoint Security.

Современные профессиональные базы данных и информационные справочные системы:

Информационно-правовая система «Консультант Плюс»;

Информационно-правовая система «Гарант»;

Электронная энциклопедия: <http://ru.wikipedia.org/wiki/Wiki>

Система комплексного раскрытия информации «СКРИН» - <http://www.skrin.ru>

Сертифицированные программные и аппаратные средства защиты информации – не предусмотрено.

Эконометрический пакет R и интерфейс RStudio или другие системы компьютерной математики (например, MAXIMA или Wolfram A).

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

Аудитории для проведения занятий.