

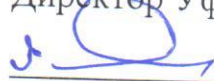
Федеральное государственное образовательное бюджетное
учреждение высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»**
(Финансовый университет)

Уфимский филиал Финуниверситета

Кафедра «Математика и информатика»

УТВЕРЖДАЮ

Директор Уфимского филиала

 Р.М. Сафуанов

« 1 » сентября 2021г.

ПРИЛОЖЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
КРИПТОГРАФИЯ И РАСПРЕДЕЛЕННЫЕ РЕЕСТРЫ

Направление подготовки 09.03.03 Прикладная информатика

Образовательная программа «Прикладная информатика»

(ИТ-сервисы и технологии обработки данных в экономике и финансах)

Год утверждения рабочей программы дисциплины: 2019

Автор рабочей программы дисциплины: Гисин В.Б.

Автор приложения к рабочей программе дисциплины: Исхаков З.Ф.

Одобрено кафедрой «Математика и информатика»

Протокол от « 30 » июня 2021 г. № 16

Содержание	Стр.
Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	4
Учебно-тематический план	5
Содержание семинаров, практических занятий	6
Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	7
Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	9
Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	9
Методические указания для обучающихся по освоению дисциплины	10
Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	10
Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	10

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

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с компетенциями/индикаторами достижения
ПКП-3	Способность применять методы разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем	1. Демонстрирует знание назначения и функционал типовых модулей корпоративных информационных систем, основные методы разработки приложений	<p>Знать: назначение и функционал типовых модулей корпоративных информационных систем в сфере экономики и финансов.</p> <p>Уметь: применять методы разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем.</p>
		2. Владеет методологией разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем	<p>Знать: методологию разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем.</p> <p>Уметь: разрабатывать приложения в сфере экономики и финансов на платформе корпоративных информационных систем.</p>

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

Очная форма обучения

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

Заочная форма обучения

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 8 (в часах)
Общая трудоемкость дисциплины	3/108	108
<i>Контактная работа - Аудиторные занятия</i>	12	12
<i>Лекции</i>	4	4
<i>Семинары, практические занятия</i>	8	8
<i>Самостоятельная работа</i>	96	96
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Экзамен	Экзамен

5.2. Учебно-тематический план

Очная форма обучения

№ п/п	Наименование темы дисциплины	Трудоёмкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа – Аудиторная работа			Самос- тоятельная работа	
			Общая, в т.ч.:	Лекции	Семинары, практические занятия		
1.	Технология распределенных реестров	18	10	4	6	8	УО, ППЗ
2.	Математические основы теории распределенных реестров	36	16	4	12	20	УО, ППЗ
3.	Криптографическ ие протоколы	34	14	4	10	20	УО, ППЗ
4.	Консенсус и время в распределенных системах	20	10	4	6	10	УО, ППЗ
	В целом по дисциплине	108	50	16	34	58	Согласно учебному плану: контрольная работа

Заочная форма обучения,

№ п/п	Наименование темы дисциплины	Трудоёмкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа – Аудиторная работа			Самос- тоятельная работа	
			Общая, в т.ч.:	Лекции	Семинары, практические занятия		
1.	Технология распределенных реестров	13	3	1	2	10	УО, ППЗ
2.	Математические основы теории распределенных реестров	33	3	1	2	30	УО, ППЗ
3.	Криптографическ ие протоколы	33	3	1	2	30	УО, ППЗ
4.	Консенсус и время в распределенных системах	29	3	1	2	26	УО, ППЗ
	В целом по дисциплине	108	12	4	8	96	Согласно учебному плану: контрольная работа

*Сокращения в таблице: УО – устный опрос; ППЗ – проверка практических заданий;

5.3. Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
Тема 1. Технология распределенных реестров	1.Распределенные реестры и блокчейн. Классификация распределенных реестров и блокчейн. Возможные применения. Безопасность. Масштабируемость. Рекомендуемые источники из раздела 8: 8.1, 8.2, 8.3, 8.4. из раздела 9: 9.1-9.10.	Интерактивная форма, Практикум по решению задач по тематике занятия в малых группах (2-4 студента) и коллективное обсуждение
Тема 2. Математические основы теории распределенных реестров	2.Топология графов. Примеры графов. Перечисление графов. Подсчет числа ребер и вершин. 3.Свойства решеток. Полное упорядочение, согласованное с частичным порядком. Теорема Дилуорта и ее следствия. Примеры решеток. Примеры векторных часов. 4,5.Алгоритмы разложения составных чисел на простые множители. Построение простых больших чисел. Освоение системы компьютерной алгебры Mathematica. Теорема Ферма. Квадратичные вычеты по простому модулю. Квадратичные вычеты по составному модулю. Тестирование чисел на простоту. Эллиптические кривые. Рекомендуемые источники из раздела 8: 8.1, 8.2, 8.3, 8.4. из раздела 9: 9.1-9.10.	
Тема 3. Криптографические протоколы.	6.Схема кодирования RSA. Протокол аутентификации. Рекомендуемые источники из раздела 8: 8.1, 8.2, 8.3, 8.4. из раздела 9: 9.1-9.10. 7.Протоколы электронно-цифровой подписи. Рекомендуемые источники из раздела 8: 8.1, 8.2, 8.3, 8.4. из раздела 9: 9.1-9.10. 8.Оценка эффективности и стойкости схем кодирования и протоколов. Рекомендуемые источники из раздела 8: 8.1, 8.2, 8.3, 8.4. из раздела 9: 9.1-9.10.	
Тема 4. Консенсус и время в распределенных системах	9.Сравнительный анализ схем консенсуса по Накамото и BFT. Рекомендуемые источники: Рекомендуемые источники из раздела 8: 8.1, 8.2, 8.3, 8.4. из раздела 9: 9.1-9.10.	

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по 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 5

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания) соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПКП-3 Способность применять методы разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем	1. Демонстрирует знание назначения и функционал типовых модулей корпоративных информационных систем, основные методы разработки приложений	Знать: назначение и функционал типовых модулей корпоративных информационных систем в сфере экономики и финансов	Типовые контрольные вопросы 1. Криптографические примитивы. 2. Односторонние функции. 3. Классы P и NP. 4. Вероятностные алгоритмы. 1. Функции хеширования.
		Уметь: применять методы разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем	Типовые контрольные задания Задание 1. Провести сравнительный анализ программных платформ «Биткоин» и «Эфириум» для создания сервиса по обмену жилыми помещениями. Задание 2. Провести сравнительный анализ стойкости ЭЦП, основанной на схеме кодирования RSA и на эллиптических кривых, опираясь на алгоритмы и значения параметров, содержащиеся в ГОСТ.
	2. Владеет методологией разработки приложений в сфере экономики и	Знать: методологию разработки приложений в сфере экономики и	Типовые контрольные вопросы . Протокол аутентификации. 9. Протокол электронной подписи на основе RSA.

	финансов на платформе корпоративных информационных систем	финансов на платформе корпоративных информационных систем	10.Группа точек на эллиптической кривой. 11.Протокол электронной подписи с использованием эллиптической кривой. 12.Скалярное время Лампорта.
		Уметь: разрабатывать приложения в сфере экономики и финансов на платформе корпоративных информационных систем.	Типовые контрольные задания Задание 1. Предположим, что агенты A_1 и A_2 передают друг другу информацию, используя систему кодирования 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. Кодировывает свое сообщение, вычисляя $c \equiv m^{e_2} \bmod N_2$; применяя функцию хеширования, вычисляет $s \equiv H(\text{hash}(m) \cdot d_1 \bmod N_1)$ 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. Задание 2. 1. Описать алгоритм работы скалярных часов Лампорта в распределенной системе. Для заданной схемы, содержащий несколько процессов (нодов) и событий, включая транзакции между нодами, расставить временные отметки, используя алгоритм Лампорта. 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 $VT_{e_i}[i] < VT_{e_j}[j]$.

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

Основная литература

1. 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 : Издательство Юрайт, 2021. — 209 с.— URL: <https://urait.ru/bcode/469567>
2. 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 : Издательство Юрайт, 2019. — 209 с. — URL: <https://urait.ru/bcode/433420>

Дополнительная литература

3. 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>
4. Гисин, В. Б. Дискретная математика : учебник и практикум для академического бакалавриата / В. Б. Гисин. — Москва : Издательство Юрайт, 2019. — 383 с. — URL: <https://urait.ru/bcode/432144> Бабичев, С. Л. Распределенные системы : учебное пособие для вузов / С. Л. Бабичев, К. А. Коньков. — Москва : Издательство Юрайт, 2020. — 507 с. — URL: <https://ezpro.fa.ru:3217/bcode/457005>

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

1. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
4. Электронно-библиотечная система Znanium <http://www.znanium.com>
5. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
6. Электронно-библиотечная система издательства Проспект <http://ebs.prospekt.org/books>
7. Электронно-библиотечная система издательства «Лань» <https://e.lanbook.com/>

8. Электронная библиотека Издательского дома «Гребенников»
<https://grebennikon.ru/>
9. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
10. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>

10. Методические указания для обучающихся по освоению дисциплины

Наименование методических материалов для обучающихся	Год утверждения	Местонахождение материала (ссылка на ИОП, информационный стенд кафедры/филиала, др.)
Методические указания к лекциям	2021	http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx
Методические указания к практическим занятиям	2021	http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx
Методические указания самостоятельной работе	2021	http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx
Методические указания к контрольной работе	2021	http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx

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:

Продукты компании Microsoft, включая ОС Windows и Office.

11.2. Современные профессиональные базы данных и информационные справочные системы

Электронное периодическое издание Справочная Правовая Система Консультант Бюджетные организации: версия Проф.

11.3 Сертифицированные программные и аппаратные средства защиты информации

Сертифицированные программные и аппаратные средства защиты информации – не используются.

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

Учебная аудитория для проведения всех видов занятий, предусмотренных программой бакалавриата, оснащенная оборудованием и техническими средствами обучения.