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

Департамент информационной безопасности

В.Б. Гисин, Е.В. Пальчевский

Криптография и распределенные реестры

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
02.03.01 Математика и компьютерные науки,
ОП «Математика и компьютерные науки»
(Компьютерные технологии анализа больших данных)

Москва 2021

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

УТВЕРЖДАЮ

Проректор по учебной
и методической работе

_____ Е.А. Каменева

«29» 06 2021 г.

В.Б. Гисин, Е.В. Пальчевский

Криптография и распределенные реестры

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки

02.03.01 Математика и компьютерные науки,

ОП «Математика и компьютерные науки»

(Компьютерные технологии анализа больших данных)

Рекомендовано Ученым советом
Факультета информационных технологий и анализа больших данных
(протокол №09 от 18.05.2021 г.)

Одобрено Советом учебно-научного
Департамента информационной безопасности
(протокол № 10 от 29.04.2021 г.)

Москва 2021

Рецензент: М.В. Коротеев, д.э.н., доцент департамента анализа данных и машинного обучения Факультета информационных технологий и анализа больших данных.

Гисин В.Б., Пальчевский Е.В. «Криптография и распределенные реестры».
Рабочая программа дисциплины для студентов, обучающихся по направлению подготовки 02.03.01 Математика и компьютерные науки, ОП «Математика и компьютерные науки» (Компьютерные технологии анализа больших данных) — М.: Финансовый университет при Правительстве Российской Федерации, Департамент информационной безопасности Факультета информационных технологий и анализа больших данных, 2021. – 23 с.

Дисциплина «Криптография и распределенные реестры» является дисциплиной Цикла профиля (элективный) по направлению подготовки 02.03.01 Математика и компьютерные науки, ОП «Математика и компьютерные науки» (Компьютерные технологии анализа больших данных).

Рабочая программа дисциплины содержит цели и задачи дисциплины, требования к результатам освоения дисциплины, содержание дисциплины, тематику практических занятий и технологии их проведения, формы самостоятельной работы студентов, систему оценивания, учебно-методическое и информационное обеспечение дисциплины.

УДК 003.26.09 (73) ББК 16.84я73

В.Б. Гисин, Е.В. Пальчевский

«Криптография и распределенные реестры»

Рабочая программа дисциплины

Компьютерный набор, верстка: Годлевский П.П.
Формат 60х90/16. Гарнитура *TimesNewRoman*.
Усл. п.л. 1,6. Изд. №– 2021. Тираж экз.
Заказ _____

Отпечатано в Финансовом университете

ОГЛАВЛЕНИЕ

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.

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПКП-4	Способность применять компьютерные технологии для анализа больших данных	1.Демонстрирует знания в области компьютерных технологий, используемых для анализа больших данных.	**1. Знать:** 1.1. Основные проблемы и направления развития аппаратных и программных средств, используемых для анализа больших данных; 1.2. Основные принципы организации и алгоритмы функционирования систем криптографии для анализа больших данных; **2. Уметь:** 2.1. Адаптировать известные методы криптографии для конкретных информационных систем с целью анализа больших данных.
		2. Выбирает компьютерные технологии в зависимости от специфики решаемых задач.	**1. Знать:** 1.1. Основные компьютерные технологии в области анализа больших данных; 1.2. Требования к алгоритмам криптографии в рамках защиты информации при анализе больших данных. **2. Уметь:** 2.1. Анализировать состав средств криптографии, обеспечивающих защиту информации при анализе больших данных; 2.2. Осуществлять выбор вида аппаратного и программного обеспечения для решения задач в области криптографии и анализа больших данных.

		3. Использует компьютерные технологии для решения прикладных задач в области анализа больших данных.	**1. Знать:** 1.1. Основные методики выбора специализированных компьютерных технологий в области анализа больших данных. **2. Уметь:** 2.1. Использовать компьютерные технологии в рамках решения различных задач в области анализа больших данных.

3. Место дисциплины в структуре образовательных программ

Дисциплина «Криптография и распределенные реестры» относится к Циклу профиля (элективный) по направлению подготовки 02.03.01 Математика и компьютерные науки, ОП «Математика и компьютерные науки» (Компьютерные технологии анализа больших данных).

Дисциплина «Криптография и распределенные реестры» базируется на знаниях, полученных в рамках изучения дисциплин «Математика», «Дискретная математика», «Информационная безопасность», «Анализ данных», «Алгоритмы и структуры данных в языке Python», входящих в образовательную программу бакалавриата по направлению подготовки 02.03.01 «Математика и компьютерные науки», профиль «Компьютерные технологии анализа больших данных».

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

Очная форма обучения, 2022 г.п. и т.д.

Вид учебной работы по дисциплине	**Всего (в з/е и часах)**	**Семестр 7 (в часах)**
Общая трудоемкость дисциплины	**3/108**	**108**
Контактная работа - Аудиторные занятия	***50***	***50***
Лекции	*16*	*16*
Семинары, практические занятия	*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 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
		Всего	Аудиторная работа				Самостоятельная работа	
			Общая, в т.ч.:	Лекции	Семинары, практические занятия	Занятия в интерактивных формах		
1.	Технология распределенных реестров	20	6	4	2	6	8	Самостоятельные работы. Участие в решении задач на практических занятиях. Собеседования по домашним заданиям.
2.	Математические основы теории распределенных реестров	36	12	4	8	12	16	
3.	Криптографические протоколы	34	26	4	22	26	22	
4.	Консенсус и время в распределенных системах	18	6	4	2	6	12	
	В целом по дисциплине	108	50	16	34	50	58	Контрольная работа
	Итого в %					100		

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

Технология распределенных реестров	1. Распределенные реестры и блокчейн. Классификация распределенных реестров и блокчейн. Возможные применения. Безопасность. Масштабируемость. *Рекомендуемые источники: п.8.[1]; п.9. [17], [18]*	Интерактивная форма, Практикум по решению задач по тематике занятия в малых группах (2-4 студента) и коллективное обсуждение решений
Математические основы теории распределенных реестров	2. Топология графов. Примеры графов. Перечисление графов. Подсчет числа ребер и вершин. *Рекомендуемые источники: 8.[2], [4]* 3. Свойства решеток. Полное упорядочение, согласованное с частичным порядком. Теорема Дилуорта и ее следствия. Примеры решеток. Примеры векторных часов. *Рекомендуемые источники: 8.[1], [2], [4]* 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. Эллиптические кривые. *Рекомендуемые источники: 8. [4]*	Интерактивная форма, Практикум по решению задач по тематике занятия в малых группах (2-4 студента) и коллективное обсуждение решений
Криптографические протоколы	6. Схема кодирования RSA. Протокол аутентификации. *Рекомендуемые источники: 8. [2], [3]; 9.[4], [5]* 7. Протоколы электронно-цифровой подписи. *Рекомендуемые источники: 8.[2], [3]; 9.[4], [5]* 8. Оценка эффективности и стойкости схем кодирования и протоколов. *Рекомендуемые источники: 8. [3]; 9. [4], [5]*	Интерактивная форма, Практикум по решению задач по тематике занятия в малых группах (2-4 студента) и коллективное обсуждение решений

Консенсус и время в распределенных системах	9. Сравнительный анализ схем консенсуса по Накамото и BFT. *Рекомендуемые источники: 9. [17], [19], [22]*	Интерактивная форма, Практикум по решению задач по тематике занятия в малых группах (2-4 студента) и коллективное обсуждение решений

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

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

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 литературой. Решение типовых задач. Разбор вопросов по теме занятия. Выполнение домашних заданий к каждому занятию.
Математические основы теории распределенных реестров	Классы сложности алгоритмов. Классы функций хеширования. Различные подходы к представлению упорядоченных множеств. Процессы в распределенных системах.	Работа с учебной литературой. Решение типовых задач. Разбор вопросов по теме занятия. Выполнение домашних заданий к каждому занятию.
Криптографические протоколы	Безопасность криптографических протоколов, утвержденных стандартами. Сравнение отечественных и зарубежных стандартов.	Работа с учебной литературой. Решение типовых задач. Разбор вопросов по теме занятия. Выполнение домашних заданий к каждому занятию.
Консенсус и время в распределенных системах	Сравнительный анализ схем консенсуса.	Работа с учебной литературой. Решение типовых задач. Разбор вопросов по теме занятия. Выполнение домашних заданий к каждому занятию.

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

Примерные вопросы к контрольной работе

1. Простые и составные числа. Разложение составных чисел на простые множители.

2. Квадратичные вычеты по простому модулю. Квадратичные вычеты по составному модулю.

3. Решение сравнений.

4. Системы линейных сравнений.

5. Функция Эйлера.

6. Эллиптические кривые.

7. Сложение точек на эллиптической кривой.

8. Циклические подгруппы группы точек эллиптической кривой.

9. Алгоритм составления электронной подписи.

10. Алгоритм проверки электронной подписи.

11. Функции хеширования.

12. Стандарты цифровой подписи.

Примеры заданий контрольной работы

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

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

1. Сформировать ключ шифрования d и ключ дешифрования (открытый ключ) $Q = d \cdot P$ в соответствии со схемой цифровой подписи ГОСТ Р34.10-2012 (ECDSA).

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

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

Данные для составления схем цифровой 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 шифрования 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).

Критерии бальной оценки различных форм текущего контроля успеваемости

Критерии бальной оценки различных форм текущего контроля успеваемости содержится в соответствующих методических рекомендациях Департамента информационной безопасности.

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

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

Типовые контрольные задания или иные материалы, необходимые для индикаторов достижения компетенций, умений и знаний

Код компетенции	Наименование компетенции	примеры заданий для оценки компетенций
ПКП-4	Способность применять компьютерные технологии для анализа больших данных	**1. Демонстрирует знания в области компьютерных технологий, используемых для анализа больших данных.** **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. Кодирует свое сообщение, вычисляя $c \equiv m^{e_2} mod\, N_2$; применяя функцию хеширования, вычисляет $s \equiv Hash(m)^{d_1} mod\, N_1$ 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.** Классы пространства имен System.Security.Cryptography.Xml могут использоваться для шифрования элементов в XML-документе. Шифрование XML-данных позволяет хранить и передавать важные XML-данные, не беспокоясь о том, что они могут быть прочитаны. При использовании симметричного алгоритма шифрования, такого как AES, также известного как алгоритм Rijndael, необходимо использовать один и тот же ключ как для шифрования, так и для

		расшифровки XML-данных. Предполагается, что зашифрованный XML-документ будет расшифровываться с помощью того же ключа, а между шифрующей и расшифровывающей сторонами существует соглашение по поводу используемых алгоритма и ключа. В этом примере в зашифрованный XML-документ ключ AES не включается (в зашифрованном или незашифрованном виде). Таким образом, необходимо зашифровать и расшифровать XML-элементы с помощью симметричного ключа **2. Выбирает компьютерные технологии в зависимости от специфики решаемых задач.** **Задание 3.** 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. 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 $VT_{e_i}[i] < VT_{e_j}[j]$. **Задание 4.** Необходимо реализовать шифрование XML-элемента с использованием двух ключей. Изначально создается пара ключей, состоящая из открытого и закрытого ключа RSA, которая сохраняется в безопасный контейнер ключа. Далее создается отдельный ключ сеанса с использованием алгоритма AES (Rijndael) для шифрования XML-документа с последующим использованием открытого ключа RSA для шифрования ключа сеанса AES. Наконец зашифрованный ключ сеанса AES и зашифрованные XML-данные сохраняются в XML-документе в новом элементе EncryptedData. Для расшифровки XML-элемента из контейнера ключа извлекается закрытый ключ RSA, который затем используется для шифрования ключа сеанса. Ключ сеанса далее используется для расшифровки документа. **3. Использует компьютерные технологии для решения прикладных задач в области анализа больших данных.** **Задание 5.**

		Необходимо прикрепить цифровую подпись к XML-документу, а затем проверить указанную цифровую подпись. Изначально создается цифровая подпись для XML-документа, которая затем прикрепляется к нему с помощью элемента Signature. Цифровая подпись представляет собой подписывающий ключ RSA, который затем добавляется в безопасный контейнер ключа и используется для подписывания XML-документа. Этот ключ может быть извлечен для проверки цифровой подписи XML, либо может использоваться для подписывания другого XML-документа.

Примеры типовых контрольных заданий

1. Построить продолжение частично порядка до линейного.

2. Построить транзитивное замыкание заданного бинарного отношения на конечном множестве.

3. Представить конечное упорядоченное множество в виде объединения непересекающихся цепей.

4. Представить конечное упорядоченное множество, используя векторные часы.

5. Вычислить значение функции Эйлера для заданного составного числа.

6. Решить систему линейных сравнений.

7. Установить, является ли заданное число квадратичным вычетом по указанному простому модулю.

8. Используя тест примарности, определить, является ли заданное число простым.

9. Оценить вероятность коллизии для заданной функции хеширования (с невысокими размерностями).

10. Выполнить сложение заданных точек указанной эллиптической кривой.

11. Провести расчеты по алгоритму кодирования Эль Гамаля.

12. Провести расчеты по протоколу аутентификации.

13. Провести расчеты по протоколу электронной подписи в схеме RSA.

14. Провести расчеты по протоколу электронной подписи, основанному на эллиптических кривых.

15. Для заданной распределенной системы, содержащий несколько процессов (нодов) и событий, включая транзакции между нодами, расставить временные отметки, используя алгоритм Лэмпорта.

Теоретические вопросы для подготовки к экзамену

1. Симметричное шифрование. Принцип Керкгофса.
2. Примеры применения криптографии. Классы атак.
3. Подстановочный шифр и его взлом.
4. Шифр Виженера, роторная машина.
5. Определение шифра. Шифр Вернама и совершенная секретность.
6. Вероятностные переформулировки совершенной секретности.
7. Эксперимент по взлому. Длина ключа в случае совершенной секретности.
8. Псевдослучайный генератор и его предсказуемость. Линейный конгруэнтный генератор.
9. Атаки на потоковые шифры.
10. Статистические тесты, преимущество. Надежность псевдослучайного генератора.
11. Непредсказуемость надежного генератора. Вычислительная неразличимость.
12. Определение схемы шифрования с закрытым ключом. Вычислительная стойкость.
13. Стойкость потокового шифра. Шифрование нескольких сообщений.
14. Стойкость относительно chosen plaintext-атак. Функции с ключом и псевдослучайные функции.
15. Шифрование с помощью псевдослучайной функции и его устойчивость.

16. Псевдослучайные перестановки. Методы работы блочных шифров.

17. Конструкции псевдослучайных перестановок. Сеть Фейстеля.

18. Аутентификация сообщений. Код аутентификации сообщений и его надежность.

19. Конструкция кода аутентификации сообщений из псевдослучайной функции.

20. Протокол интерактивного обмена ключами, его надежность. Описание протокола Диффи– Хеллмана.

21. Задача DDH и надежность протокола Диффи–Хеллмана.

22. Схема шифрования с открытым ключом, ее надежность относительно подслушивания и относительно chosen plaintext-атак.

23. Шифрование нескольких сообщений, его надежность. Гибридное шифрование.

24. Наивная схема шифрования RSA. Ускорение дешифровки, маленький показатель.

25. RSA с набивкой, задача RSA и надежность схемы шифрования RSA с набивкой.

26. Схема Эль-Гамаля и ее надежность.

27. Квадратичные вычеты и символ Якоби.

28. Задача определения квадратичных вычетов и схема шифрования Гольдвассер–Микали.

29. Извлечение квадратных корней и схема шифрования Рабина.

30. Остатки по модулю N2 и схема шифрования Пайе.

31. Схема цифровой подписи, ее надежность. Наивная схема RSA.

32. RSA с хэшем. Схема одноразовой подписи Лэмпорта.

33. Доказательства с нулевым разглашением.

34. Сертификаты. Схемы разделения секрета.

35. Основные понятия криптографии.

36. Блочные и поточные шифры.

37. Понятие криптосистемы.

38. Ручные и машинные шифры.

39. Основные требования к шифрам.

40. Криптосистемы RSA и Эль-Гамаля.

Примеры 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 Информационной безопасности
Форма обучения: очная Семестр: 7
Направление подготовки: **02.03.01 Математика и компьютерные науки**
Профиль: Компьютерные технологии анализа больших данных

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №

1. Основные понятия криптографии. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Основные требования к шифрам. (20 баллов)
2. Криптосистемы RSA и Эль-Гамаля. (20 баллов)
3. Реализовать шифрование XML-файла с помощью симметричного и ассиметричного методов шифрований. (20 баллов)

Подготовил: Пальчевский Е.В.

Утверждаю:
Первый заместитель
руководителя департамента _____Феклин В.Г.

_____ Дата

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

Основная литература:

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

5. Peter, H. Gregory Blocking Spam For Business For Dummies® (For Dummies (Computers)) / Peter H. Gregory. - Москва: ИЛ, 2016. - 636 с.

6. Бабаш, А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2016. - 240 с.

7. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - 376 с.

8. Бабенко, Л.К. Современные интеллектуальные пластиковые карты / Л.К. Бабенко. - М.: Гелиос АРВ, 2015. - 921 с.

9. Криптография: скоростные шифры / А. Молдовян и др. - М.: БХВ-Петербург, 2014. - 496 с.

10. Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2013. - 192 с.

11. Литвинская, О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. - М.: КноРус, 2015. - 168 с.

12. Осмоловский, С. А. Стохастическая информатика. Инновации в информационных системах / С.А. Осмоловский. - М.: Горячая линия - Телеком, 2012. - 322 с.

13. Стохастические методы и средства защиты информации в компьютерных системах и сетях: моногр. / Под редакцией И.Ю. Жукова. - М.: КУДИЦ-Пресс, 2016. - 512 с.

14. Хоффман, Л. Дж. Современные методы защиты информации / Л.Дж. Хоффман. - Москва: СПб. [и др.] : Питер, 2014. - 264 с.

15. Шаньгин, В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - Москва: Огни, 2016. - 551 с.

16. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. - М.: Триумф, 2012. - 518 с.

17. Шумский, А.А. Системный анализ в защите информации / А.А. Шумский. - Москва: СПб. [и др.] : Питер, 2013. - 224 с.

Дополнительная литература:

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

9. 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://librarry.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.znanium.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-tekhnologia-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

10. 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.

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

11.1. Комплект лицензионного программного обеспечения:

− Windows, Microsoft Office, Chrome

− Программное обеспечение антивирусной защиты компьютера.

11.2 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.

11.3. Сертифицированные программные и аппаратные средства защиты информации – не предусмотрено.

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

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

1. Компьютерные классы с набором лицензионного базового программного обеспечения для проведения практических занятий и выходом в глобальную сеть Internet.

2. Лекции с применением мультимедийных материалов, мультимедийная аудитория.