МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Руководитель образовательной программы
_____ / Сесин А.В.
«5» марта 2021г.

Фонд оценочных средств

Код модуля	Модуль
1156691	Компьютерные и информационные технологии в технике и экономике

Екатеринбург, 2021

Фонд оценочных средств составлен авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра
1	Сесекин Александр Николаевич	д-р физ.-мат. наук, профессор	профессор	прикладной математики
2	Гредасова Надежда Викторовна	канд. физ.-мат. наук	доцент	прикладной математики
3	Костоусов Виктор Борисович	кандидат физико-математических наук, доцент	доцент	прикладной математики и механики

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры «Прикладная математика»

И.о.зав. кафедрой «Прикладная математика» Н.В. Гредасова

Протокол № 1 от 05.03.21 г.

1. Критерии и шкалы оценивания компетенций

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации

Шкала оценивания		Критерии оценивания	Уровни освоения компетенций
«отлично» (80-100 баллов)	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Продемонстрировал владение профессиональным языком в определенной предметной области. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо» (60-79 баллов)		Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Повышенный
«удовлетворительно» (40-59 баллов)		Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе	Пороговый

		на дополнительные вопросы	
«неудовлетворительно» (менее 40 баллов)	«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

Критерии и шкалы оценивания результатов обучения при проведении текущей аттестации представлены в «Методических рекомендациях по критериям и шкалам оценивания в рамках БРС».

2. Оценочные средства для проведения текущей и промежуточной аттестации

Дисциплина «Защита информации»

2.1. Примерные задания для проведения контрольной работы

1. Найти все **первообразные** корни меньше M={5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 43} т.е. найти образующие элементы мультипликативной группы кольца вычетов по модулю M
2. **Выполнить тесты н**а простоту числа следующих бинарных величин (hexadecimal, little endian):
   - 7a3c76ed
   - 6e31c8aad4233546
   - 80e081c50947a63d1a9d20778be195c1
   - cea7170bff0d57299989119f3f75dfa3c6d794d544dc65a15ad8edd5e5d64113
   - 7656366f73f5c5b090bb1783da52444119c37acc932719e097c9a71140fb4e01561cae0a9ee37130781680a89f2f2800919c6de2c3fe0e7855f64cdf79ff9ef7
3. Извлечь квадратный корень из чисел 11, 19, 51, 101, 113, 121, 179, 241 по модулю 317
4. Вычислить открытый ключ E криптосистемы RSA, связанному с приватным ключом D = 113 для значений модуля N1 = 127, N2 = 191, N3 = 331

Для контроля использовать программы: PARI/GP, OpenSSL

2.2. Примерные задания для проведения домашней работы

1. Найти условия публичного ключа E и модуля N в криптосистеме RSA для получения исходного сообщения через M последовательных шифрований

2.3. Перечень примерных вопросов для зачета

1. Концепция информационной безопасности.
2. Виды угроз. Внутренние и внешние источники угроз.
3. Организационно-правовое обеспечение информационной безопасности.
4. Угрозы в информационных системах.
5. Способы защиты информации.
6. Средства защиты информации.
7. Компьютерные вирусы и антивирусные программы.
8. Государственные стандарты по информационной безопасности.
9. Понятие информационной безопасности. Угрозы. Механизмы анализа угроз. Инструментарий построения рубежей.
10. Основы криптографии. Шифрование и кодирование. Общие принципы и модели.
11. Защита от несанкционированного доступа.

12. Простые шифры. Шифр простой замены. Шифр Цезаря (шифр сдвига, код Цезаря, сдвиг Цезаря).
13. Шифр вертикальной перестановки (перестановочный шифр, шифрограмма по вертикалям).
14. Гаммирование (метод симметричного шифрования).
15. Методы расшифровки зашифрованной информации. Основные способы криптоанализа простых шифров.
16. Основные методы криптоанализа. Атака на основе шифротекста, открытых текстов и соответствующих шифротекстов, подобранного открытого текста, адаптивно подобранного открытого текста.
17. Дополнительные методы криптоанализа. Атака на основе подобранного шифротекста, подобранного ключа. Бандитский криптоанализ
18. Симметричные криптосистемы. Схема, сеть Фейстеля (Horst Feistel, Feistel network, Feistel cipher). Стандарты блочного шифрования. Федеральный стандарт DES.
19. Симметричные криптосистемы. Алгоритм шифрования ГОСТ 28147-89 (Магма), ГОСТ Р 34.12-2015 (Кузнечик). режимы шифрования и гаммирования.
20. Симметричные криптосистемы. Алгоритм блочного шифрования Rijndael - Advanced Encryption Standard (AES).
21. Атаки на блочные шифры. Дифференциальный криптоанализ. Дифференциальный криптоанализ на основе отказов устройства.
22. Атаки на блочные шифры. Линейный криптоанализ. Силовая атака на основе распределенных вычислений.
23. Поточные шифры. Регистры сдвига с обратной связью. Алгоритм поточного шифрования RC4 (Rivest cipher 4, Ron’s code; ARC4, ARCFOUR).
24. Основные теоремы теории чисел. Проверка числа на простоту. Эффективные алгоритмы возведения в степень.
25. Криптосистема RSA (Rivest-Shamir-Adleman — криптографический алгоритм с открытым ключом). Устройство RSA. Эффективность реализации. Криптостойкость RSA.
26. Атаки на криптосистему RSA. Атака на основе выбранного шифр текста. Атака на основе общего RSA модуля. Раскрытие малого показателя шифрования.
27. Криптосистема Эль-Гамаля (Elgamal). Вычисление и проверка подписи. Шифрование и дешифрование. Эффективность реализации.
28. Метод экспоненциального ключевого обмена Диффи-Хелмана. Протокол ключевого обмена для нескольких участников.
29. Хеш-функции. Понятие хеш-функции. Основные свойства односторонних функций. MD4 (Message Digest 4), RFC 1186 (The MD4 Message Digest Algorithm).
30. Цифровая подпись. Понятие цифровой подписи. Основные принципы и отличия от реальной подписи. Алгоритмы цифровой подписи - ГОСТ Р 34.10-2012. DSS (Digital Signature Standard).
31. Закон об эектронной цифровой подписи в России. Удостоверяющие центры.
32. Протоколы генерации ключей. Случайные ключи. Протоколы распределения ключей.
33. Разделение секрета. Схема разделения секрета Шамира.
34. Применение помехоустойчивых кодов в криптографии. Недвоичные циклические коды Рида-Соломона(Reed–Solomon codes).
35. Верифицируемое разделение секрета.
36. «Шарады» с временным замком (Time-lock puzzles and timed-release Crypto). Построение «шарад» с временным замком. Решение «Шарады»
37. Квантовая криптография - основанная на принципах квантовой физики. Квантовый протокол распределения ключей. Распределение ключей в оптических сетях.
38. Криптографические протоколы: обеспечение различных режимов аутентификации; генерация, распределение и согласование криптографических ключей; защита взаимодействий участников; разделение ответственности между участниками.

39. Доказательство принадлежности (Zero-knowledge proof). Доказательство при отказе отправителя. Доказательство при отказе получателя.
40. Нормативно-правовое обеспечение информационной безопасности.
41. Классификация секретной информации в России. Служебная, коммерческая и государственная тайны.
42. Законы РФ: «Информации, информатизации и защите информации»; Закон о персональных данных; ...
43. Стандарты ИБ: ISO/IEC 15408; руководящие документы ФСТЭК; Оранжевая книга (Критерии определения безопасности компьютерных систем - Trusted Computer System Evaluation Criteria; Радужная серия).
44. Политика безопасности. Уровень гарантированности. Классы безопасности. Безопасность распределенных систем. Рекомендации X.800.
45. Роли и ответственности субъектов информационного пространства. Принцип распределения ответственности. Матрица распределения доступа для сотрудников организации.
46. Понятие управления рисками. Качественные и количественные методики оценки рисков. Количественная модель рисков QRM (Quantitative Risk Model). Оценки по конфиденциальности информации.
47. Политика информационной безопасности. Цели и задачи организации. Взаимодействие между субъектами. Правила безопасности.
48. Политика информационной безопасности для локальной вычислительной сети.

2.4. Задания, по которым проводится аттестация, оформляются и хранятся в составе ФОС согласно установленным требованиям (Положение о ФОС) и не размещаются в электронной информационно-образовательной среде УрФУ.

Дисциплина «Параллельное и распределенное программирование»

2.1. Примерные задания для проведения контрольной работы

1. Сгенерировать две матрицы размерностью NxM и MxK (N, M, K > 1000). Написать параллельную программу умножения двух матриц с использованием технологии CUDA/OpenMP. Реализовать ту же программу без применения параллельного подхода и составить сравнительный анализ.

2. Сгенерировать случайный массив размерностью N (N > 2 млн.). Написать параллельную программу для поиска максимального элемента в массиве с использованием технологии CUDA/OpenMP. Реализовать ту же программу без применения параллельного подхода и составить сравнительный анализ.

2.2. Примерные задания для проведения домашней работы

1. Сгенерировать случайный массив размерностью N (N > 2 млн.). Написать параллельную программу для сортировки массива с использованием технологии OpenMP. Реализовать ту же программу без применения параллельного подхода и составить сравнительный анализ.

2. Написать параллельную программу для разложения Холецкого.

2.3. Примерные задания для проведения курсовой работы

1. Написать параллельную программу для решения СЛУ вида Ax = b. Построить сравнительный анализ параллельной и последовательной реализаций.

2. Написать параллельную программу для выделения границ объектов на изображении. Построить сравнительный анализ параллельной и последовательной реализаций.

3. Написать параллельную программу для реализации алгоритма Флойда. Построить сравнительный анализ параллельной и последовательной реализаций.

2.4. Перечень примерных вопросов для экзамена

1. Цели и задачи параллельной обработки данных. Необходимость и актуальность параллельных вычислений.
2. Различия между многозадачным, параллельным и распределенным режимами выполнения программ. Закон Амдаля. Закон Мура. Гипотеза Минского.

3. Способы построения многопроцессорных вычислительных систем. Краткая история развития высокопроизводительных вычислений.
4. Рейтинги ведущих суперкомпьютеров: мировой TOP-500, TOP-50 СНГ
5. Систематика Флинна. Детализация систематики Флинна.
6. Понятия мультипроцессора, мультикомпьютера, вычислительного кластера. Особенности организации параллельных вычислений в системах с общей памятью (обеспечение однозначности кэш-памяти разных процессоров, синхронизация вычислений).
7. Особенности организации параллельных вычислений в системах с распределенной памятью посредством передачи сообщений. Топологии сетей передачи данных в мультикомпьютерах.
8. Понятие кластера и кластерной архитектуры. Классификация кластерных вычислительных систем. Состав сетевой инфраструктуры кластера. Типы топологий и критерии эффективности коммуникационной сети кластера.
9. Сетевые решения для кластерных систем.
10. Особенности запуска задач на кластерах.
11. Показатели эффективности параллельного алгоритма и оценка максимально достижимого параллелизма.
12. Параллелизм на примере модельных задач нахождения частных сумм последовательности числовых значений и умножения матриц.
13. Общая схема и методика разработки параллельных алгоритмов.
14. Общая характеристика методов передачи данных, оценка времени выполнения коммуникационных операций.
15. Оценка трудоемкости операций передачи данных для кластерных систем. Модель Хокни. MPI: основные понятия и определения. Базовый (минимальный) набор функций MPI, достаточный для разработки параллельных программ.
16. Операции передачи данных между двумя процессами
17. Общие сведения. Структура стандарта OpenMP. Достоинства технологии OpenMP. Модель параллелизма OpenMP.
18. Модель памяти OpenMP. Директивы OpenMP. Типы директив. Формат записи директив. Определение параллельной области. Распределение вычислений между потоками.
19. Директивы синхронизации. Директивы управления областью видимости данных. Совместимость директив и их параметров. Библиотека функций OpenMP.
20. DVM-система. Общие сведения, цели создания, принципы построения. Модель параллелизма, модель выполнения и модель программирования DVM.
21. Языки программирования DVM. Директивы DVM (на примере языка C-DVM). Сравнение размеров и эффективности MPI- и DVM-программ.
22. Переносимость и повторное использование DVM-программ.

3.5. Задания, по которым проводится аттестация, оформляются и хранятся в составе ФОС согласно установленным требованиям (Положение о ФОС) и не размещаются в электронной информационно-образовательной среде УрФУ.

Дисциплина «Распознавание образов»

2.1. Примерные задания для проведения контрольной работы

Разработка программного модуля решающих правил системы распознавания лиц. Для получения доступа к фрагменту изображения лица используется встроенный обнаружитель лиц ofxCvHaarFinder, входящий в библиотеки OpenFrameWorks и OpenCV, основанный на каскадном классификаторе, составленном из признаков Хаара. Для получения обучающей выборки используется пространство геометрических, яркостных и текстурных признаков.

Решающие правила формируются на основе обучения

для <u>темы № 1</u>:

одиночного персептрона Розенблатта;

для <u>темы № 2</u>:

нелинейного классификатора SVM – машины опорных векторов.

для <u>темы № 3</u>:

метода главных компонент (PCA), примененного к нормированному яркостному вектору.

Тема № 4. Построение ROC-кривой для линейного классификатора и оценка качества обучения персептрона Розенблатта.

Программа должна быть обеспечена средствами визуализации входных и выходных данных, с использованием библиотек OpenFrameWorks и OpenCV. Программирование может осуществляться на языках C++ (MS Visual Studio 7 и выше), Pithon и Java.

2.2. Примерные задания для проведения домашней работы

Разработка программного модуля системы распознавания лиц, предназначенного для преобразования исходного изображения в пространство признаков. Для получения доступа к фрагменту изображения лица используется встроенный обнаружитель лиц ofxCvHaarFinder, входящий в библиотеки OpenFrameWorks и OpenCV, основанный на каскадном классификаторе, составленном из признаков Хаара.

Пространство признаков определяется из заданного перечня, который включает:

для темы №1:

геометрические характеристики:

- внешний контур лица;
- положение ключевых точек лица: уголки глаз, губ, кончик носа, центр глаза и т. п.
- расстояния между ключевыми точками лица
- положение и размеры ключевых областей: глаза, нос, рот

для темы №2:

яркостные характеристики:

- средняя нормированная яркость в окрестности
- локальные пороговые яркости (бинарный вектор)

для темы №3:

текстурные характеристики Харалика

Программа должна быть обеспечена средствами визуализации входных и выходных данных, с использованием библиотек OpenFrameWorks и OpenCV. Программирование может осуществляться на языках C++ (MS Visual Studio 7 и выше), Pithon и Java.

2.3. Перечень примерных вопросов для экзамена

1. Основные понятия и определения математической теории распознавания образов
2. Байесов классификатор.
3. Алгоритм ближайшего соседа, k ближайших соседей, взвешенных соседей.
4. Обучение без учителя, кластеризация. Метод k-средних.
5. Метод главных компонент
6. Многослойные нейронные сети Метод обратного распространения ошибок
7. Преобразование Хафа и обобщённое преобразование Хафа
8. Сопоставление с эталоном методом корреляции
9. Понятие оптического потока. Метод Люкаса-Канаде.

2.4. Задания, по которым проводится аттестация, оформляются и хранятся в составе ФОС согласно установленным требованиям (Положение о ФОС) и не размещаются в электронной информационно-образовательной среде УрФУ.

Дисциплина «Информационные технологии анализа данных»

2.1. Перечень примерных вопросов для зачета

1. Основные библиотеки языка Python.
2. Логические методы классификации.
3. Метрические методы классификации.
4. Линейные метод опорных векторов и логистическая регрессия.
5. Метрика качества классификации.

6. Линейная регрессия.
7. Понижение размерности и метод главных компонент.
8. Композиции алгоритмов.
9. Нейронные сети.
10. Кластеризация и визуализация.
11. Частичное обучение.
12. Машинное обучение в прикладных задачах.

2.2. Задания, по которым проводится аттестация, оформляются и хранятся в составе ФОС согласно установленным требованиям (Положение о ФОС) и не размещаются в электронной информационно-образовательной среде УрФУ.