Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 01.04.02 Прикладная математика и информатика

Наименование образовательной программы: Математическое моделирование

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Методы защиты информации и распознавания образов

Москва
2021

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Фролов А.Б. Идентификатор: Ref8507cb-FrolovAB-a54b01e2	А.Б. Фролов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Черепова М.Ф. Идентификатор: R9267877e-CherepovaMF-dbb9bf1	М.Ф. Черепова
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Зубков П.В. Идентификатор: R4920bc6f-ZubkovPV-8172426c	П.В. Зубков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-1 Способен создавать, исследовать и реализовывать математические модели естествознания и технологий

ИД-3 Демонстрирует знание терминологии, основных понятий и методов решения прикладных задач

ИД-5 Применяет современные методы исследования математических моделей

ИД-6 Разрабатывает и исследует алгоритмы численного решения прикладных задач

ИД-7 Анализирует результаты численного и аналитического решения прикладных задач

и включает:

для текущего контроля успеваемости:

Форма реализации: Билеты (письменный опрос)

1. Алгоритмы кластеризации, классификации и ранжирования (Контрольная работа)
2. Библиотеки программ для распознавания и анализ работы поискового робота (Контрольная работа)
3. Блочные системы шифрования (Контрольная работа)
4. Криптосистемы с открытым ключом (Контрольная работа)
5. Методы распознавания частично-упорядоченных объектов и принцип конечной топологии (Контрольная работа)
6. Принципы классификации и распознавания в метрических пространствах (Контрольная работа)
7. Электронная цифровая подпись (Проверочная работа)

Форма реализации: Защита задания

1. Распределение ключей в компьютерной сети (Расчетно-графическая работа)

БРС дисциплины

2 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Задачи защиты информации криптографическими методами и виды атак					
Задачи защиты информации криптографическими методами и виды атак		+			
Распределение ключей в компьютерной сети. Разделение секрета					

Распределение ключей в компьютерной сети. Разделение секрета	+			
Блочные системы шифрования				
Блочные системы шифрования		+		
Хеш-функции и их применение				
Хеш-функции и их применение		+		
Криптосистемы с открытым ключом				
Криптосистемы с открытым ключом			+	
Протоколы с нулевым разглашением секрета				
Протоколы с нулевым разглашением секрета			+	
Электронная цифровая подпись				
Электронная цифровая подпись				+
Протоколы, основанные на спаривании				
Протоколы, основанные на спаривании				+
Вес КМ:	25	25	25	25

3 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-5	КМ-6	КМ-7	КМ-8
	Срок КМ:	4	8	12	15
Классификация и распознавание в метрических пространствах					
Классификация и распознавание в метрических пространствах		+			
Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов					
Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов			+	+	
Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм					
Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм					+
Вес КМ:		25	25	25	25

$Общая часть/Для промежуточной аттестации$

БРС курсовой работы/проекта

3 семестр

Раздел дисциплины	Веса контрольных мероприятий, %

	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Изучение материалов		+			
Разработка плана программы			+		
Составление программы				+	
Отладка программы					+
	Вес КМ:	25	25	25	25

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-1	ИД-3$_{ПК-1}$ Демонстрирует знание терминологии, основных понятий и методов решения прикладных задач	Знать: основные атаки на криптографические протоколы модели шифров симметричных криптосистем и криптосистемы с открытым ключом алгоритмы кластеризации, классификации и ранжирования методы распознавания частично-упорядоченных объектов и принцип конечной топологии принципы классификации и распознавания в метрических пространствах Уметь: анализировать структуру блочного шифра	Блочные системы шифрования (Контрольная работа) Криптосистемы с открытым ключом (Контрольная работа) Принципы классификации и распознавания в метрических пространствах (Контрольная работа) Алгоритмы кластеризации, классификации и ранжирования (Контрольная работа) Методы распознавания частично-упорядоченных объектов и принцип конечной топологии (Контрольная работа)
ПК-1	ИД-5$_{ПК-1}$ Применяет современные методы	Уметь: применять готовые	Библиотеки программ для распознавания и анализ работы поискового робота (Контрольная работа)

	исследования математических моделей	библиотеки программ для распознавания и анализировать работу поискового робота	
ПК-1	ИД-6$_{ПК-1}$ Разрабатывает и исследует алгоритмы численного решения прикладных задач	Знать: российские криптографические стандарты Уметь: создавать исполнимые спецификации криптографических протоколов	Распределение ключей в компьютерной сети (Расчетно-графическая работа) Электронная цифровая подпись (Проверочная работа)
ПК-1	ИД-7$_{ПК-1}$ Анализирует результаты численного и аналитического решения прикладных задач	Уметь: анализировать стойкость схем шифрования	Криптосистемы с открытым ключом (Контрольная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

2 семестр

КМ-1. Распределение ключей в компьютерной сети

Формы реализации: Защита задания
Тип контрольного мероприятия: Расчетно-графическая работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Самостоятельное выполнение четырех задач с индивидуальными исходными данными с представлением откомментированного по результатам анализа листинга их компьютерного исполнения.

Краткое содержание задания:

1. Расчетное задание на тему «Распределение ключей в компьютерной сети» связано с проверкой умения создавать исполнимые спецификации криптографических протоколов

Контрольные вопросы/задания:

Уметь: создавать исполнимые спецификации криптографических протоколов	1.С использованием Алгебраического процессора составить и протестировать исполнимую спецификацию протокола Месси-Омуры. 2.С использованием Алгебраического процессора составить и протестировать исполнимую спецификацию протокола Диффи-Хелмана с атакой “человек посередине” на этот протокол. 3.С использованием Алгебраического процессора составить и протестировать исполнимую спецификацию протокола RSA с атакой по выбираемому шифр тексту. 4.С использованием Алгебраического процессора составить и протестировать исполнимую спецификацию протокола Диффи-Хелмана с аутентификацией.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если задание выполнено в полном объеме или выполнено преимущественно верно.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если большинство вопросов раскрыто. выбрано верное направление для решения задач.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если задание преимущественно выполнено

КМ-2. Блочные системы шифрования

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный опрос проводится по вариантам. Билет содержит 4 задания на 20 минут

Краткое содержание задания:
Контрольная работа по теме по теме «Блочные системы шифрования» связана с проверкой знания основных атак на криптографические протоколы и умения анализировать структуру блочного шифра

Контрольные вопросы/задания:

Знать: основные атаки на криптографические протоколы	1.Как организуется атака по выбираемому шифру RSA 2.Как организуется атака по выбираемому шифру Рабина 3.Как организуется атака на криптосистему RSA встречей посередине 4.Какое свойство криптосистемы RSA влечет успех атаки по выбираемому шифртексту 5.Перечислите принципы блочного шифрования 6.Каковы функции сети Фейстеля 7.Покажите, что различным наборам значений сигналов на входе блока расширения DES соответствуют различные наборы значений выходных сигналов этого блока 8.Каково назначение блоков S в сети Фейстеля
Уметь: анализировать структуру блочного шифра	1.Каково назначение блоков S в сети Фейстеля 2. Перечислите общие особенности стандартов шифрования DES и ГОСТ28147-89 и специфику реализации каждого из них 3.Каковы общие режимы использования блочных шифров DES и ГОСТ28147-89 и какие режимы являются специфическими 4.В чем состоит ограничение применения режима кодовой книги (шифра простой замены) 5.Как осуществляется аутентификация с использованием блочных шифров. 6.Какой параметр блочного шифра определяется гарантированным периодом гаммы 7.В чем состоит опасность режима сцепления блоков?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка 5 выставляется при полном ответе на теоретические вопросы и при решении обеих задач, возможно с несущественными ошибками.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 4 выставляется про полном ответе на теоретические вопросы и при решении одной задач, но при отсутствии решения второй задачи.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 выставляется при полном ответе на один теоретический вопрос и решении одной задачи.

КМ-3. Криптосистемы с открытым ключом

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный опрос проводится по вариантам. Билет содержит 4 задания на 20 минут

Краткое содержание задания:
Контрольная работа по теме «Криптосистемы с открытым ключом» связан с проверкой знания моделей шифров симметричных криптосистем и криптосистем с открытым ключом и умения анализировать стойкость систем шифрования.

Контрольные вопросы/задания:

Знать: модели шифров симметричных криптосистем и криптосистемы с открытым ключом	1.В какой алгебраической системе выбираются основные параметры RSA 2.В какой алгебраической системе выбираются экспоненты RSA? 3.Почему пользователи компьютерной сети не должны при выборе основных параметров RSA применять одинаковые модули? 4.Каким необходимым свойством цифровой подписи не обладает подпись RSA (показать, почему нет этого свойства RSA)? 5.Как строится атака на RSA по выбираемому шифртексту и какое свойство RSA при этом используется? 6.Как строится атака встречей посередине на RSA и какое свойство RSA при этом используется? 7.На какой трудной проблеме теории чисел основана безопасность криптосистемы Рабина? 8.Какие предосторожности следует соблюдать при выборе параметров криптосистемы Рабина? 9.Какова сложность алгоритмов зашифрования и расшифрования криптосистемы Рабина? 10.Возможно ли шифрование блоков текстов на естественном языке посредством криптосистемы Рабина без введения дополнительной избыточности?

	11.Какой трудной проблеме теории чисел соответствует безопасность криптосистемы Эль Гамаля? 12. Какие предосторожности следует соблюдать при выборе параметров криптосистемы Эль Гамаля? 13.Почему недопустимо повторное использование рандомизатора? 14.На какой трудной теоретико-числовой проблеме основана криптографическая стойкость криптосистемы Гольдвассер --- Микали? 15. На каком основании криптосистема Гольдвассер -- Микали считается семантически секретной, 16.С какой целью в криптограмму, получаемую в криптосистеме Блюма ---Гольдвассер добавляется в конце шифртекста x_{t+1}? 17.Покажите, что криптосистемы RSA, Рабина, Эль Гамаля, Гольдвассер --- Микали и Блюма --- Гольдвассер не стойки против атак по выбираемому шифртексту. 18.Какова цель протокола с нулевым разглашением секрета и какова структура итерации такого протокола? 19.Как характеризуются полнота и устойчивость протокола с нулевым разглашением секрета, каковы области значений этих характеристик? 20.Почему в протоколах с нулевым разглашением секрета предусматривается два типа вопросов? 21.Чем обеспечивается свойство нулевого разглашения секрета? 22.Из каких соображений выбирают количество итераций протокола с нулевым разглашением секрета? 23. Какие сложные проблемы теории чисел лежат в основе безопасности протоколов доказательства знания дискретного логарифма и протокола Фиата-Шамира? 24. Каким преимуществом обладает протокол Шнорра? 25.Какие протоколы с нулевым разглашением секрета называются совершенными?
Уметь: анализировать стойкость схем шифрования	1.Вычислить секретный ключ криптосистемы RSA при заданных модуле n и экспоненте зашифрования e, если известна другая пара таких экспонент при том же модуле n, не прибегая к разложению модуля n. 2.Разложить модуль n криптосистемы RSA при известных экспонентах e зашифрования и расшифрования d. 3.Получить экспоненту расшифрования криптосистемы RSA методом встречи посередине. 4.Вскрыть криптосистему RSA с модулем 4757. 5.Получить сообщение m по его криптограмме Эль Гамаля (C_1,C_2), если известна криптограмма (C_1,

	C'_2) сообщения m'.. 6.Решить проблему Диффи-Хеллмана с помощью оракула Эль Гамаля (возвращающего сообщение из крипторамы Эль гамаля). 7.Смоделировать атаку по выбираемому шифртексту на криптосистему Гольдвассер-Микали. 8.Построить модель, показывающую, что протокол Шнорра совершенный. 9.Построить подписанное ключом RSA сообщение.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка 5 выставляется про полном ответе на теоретические вопросы и при решении одной задач, но при отсутствии решения второй задачи.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 4 выставляется про полном ответе на теоретические вопросы и при решении одной задач, но при отсутствии решения второй задачи.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 выставляется при полном ответе на один теоретический вопрос и решении одной задачи.

КМ-4. Электронная цифровая подпись

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Проверочная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный опрос проводится по вариантам. Билет содержит 4 задания на 20 минут

Краткое содержание задания:

1. Проверочная работа по теме «Электронная цифровая подпись». связана с проверкой знания российских криптографических стандартов.
2.

Контрольные вопросы/задания:

Знать: российские криптографические стандарты	1. 1. Перечислите основные свойства цифровой электронной подписи. 2.Каким свойством не обладает цифровая подпись на основе криптосистемы с открытым ключом? 3.Какой трудной проблеме эквивалентна стойкость цифровой подписи Эль-Гамаля? 4.Почему недопустимо повторное использование рандомизатора при формировании цифровой подписи

	Эль-Гамаля? 5.К чему приведет игнорирование проверки принадлежности первого числа цифровой подписи Эль-Гамаля мультипликативной группе, на которой она определена? 6.В чем смысл применения хеширования при образовании цифровой подписи Эль-Гамаля? 7.В чем сходство и в чем различие российского и американского стандартов стандартов цифровой подписи в мультипликативной группе? 8.В чем различие системы сертификации открытого ключа и системы, основанной на использовании личностного ключа? 9.В чем состоят преимущества и недостатки системы цифровой подписи с личностным ключом по сравнению с системой, использующей сертифицированный ключ проверки? 10.Покажите, что предикат проверки подписи принимает значение True, если сообщение подписано владельцем секретного ключа. 11.К каким последствиям может привести коллизия хэш-функции, т.е. если случится, что h(t||M)= h(t||M'), где M' - фальсифицированное сообщение? 12.Какие предосторожности следует соблюдать при выборе параметров системы с личностным ключом? 13.Какова особенность цифровой подписи с возвратом сообщения? 14.Как формируется ключ проверки подписи с личностным ключом? 15.Является ли цифровая подпись с личностным ключом эксклюзивной подписью участника? 16.В чем преимущество использования группы точек эллиптической кривой по сравнению с использованием мультипликативной группы? 17.Российский стандарт цифровой подписи ГОСТ Р 34.10-94. 18.Цифровая подпись с возвратом сообщения. Электронная подпись ГОСТ Р. 34.10-2012.

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка 5 выставляется про полном ответе на теоретические вопросы и при решении одной задач, но при отсутствии решения второй задачи.

Оценка: 4

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Оценка 4 выставляется про полном ответе на теоретические вопросы и при решении одной задач, но при отсутствии решения второй задачи.

Оценка: 3

Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 выставляется при полном ответе на один теоретический вопрос и решении одной задачи.

3 семестр

КМ-5. Принципы классификации и распознавания в метрических пространствах

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проводится на практическом занятии, продолжительность выполнения работы 40 минут. Студентам выдаётся несколько вариантов заданий

Краткое содержание задания:
В работе проверяется знание принципов классификации и распознавания в метрических пространствах

Контрольные вопросы/задания:

Знать: принципы классификации и распознавания в метрических пространствах	1.Что такое гипотеза компактности? 2.Перечислите четыре вида мер сходства 3.Что такое линейная решающая функция? 4.Приведите пример выборки, для которой нельзя построить линейную разделяющую гиперплоскость 5.Что такое персептрон? 6.Приведите пример обучения с учителем 7.Приведите пример обучения без учителя 8.Что понимается под термином точность при оценке качества классификации? 9.Приведите пример предварительной обработки образов 10.Приведите пример малозначимого признака 11.Приведите пример преобразование кластеров

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-6. Библиотеки программ для распознавания и анализ работы поискового робота

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проводится на практическом занятии, продолжительность выполнения работы 40 минут. Студентам выдаётся несколько вариантов заданий

Краткое содержание задания:
В работе проверяется умение применять готовые библиотеки программ для распознавания и анализировать работу поискового робота

Контрольные вопросы/задания:

Уметь: применять готовые библиотеки программ для распознавания и анализировать работу поискового робота	1.Запишите команду, определяющую массив Numpy, состоящий из элементов 0,1,2,3,4,5. 2.Запишите команду для вывода на экран изображения image с помощью библиотеки matplotlib 3.Запишите команду, добавляющую в модель нейронной сети, составленную с помощью библиотеки keras, полносвязный слой с размерностью выходного пространства 10 и функцией активации softmax 4.Запишите команду для прогноза значения переменной y_model по экспериментальным данным, представленным переменной Xtest, использующую уже обученную на данных обучающей выборки модель model, созданную с помощью библиотеки scikit-learn 5.Запишите команду для подключения модуля nn из библиотеки PyTorch 6.Составьте два предложения, являющиеся релевантным и нерелевантным ответом на запрос "знак точка с запятой" 7.Составьте два предложения, в которых частота употребления слова “привет” разная 8.Составьте таблицу, по вертикали которой будут выписаны 3 первых сайта из выдачи поисковой системы по запросу “сложение матриц”, а по горизонтали факторы ранжирования, которые Вы считаете повлиявшими на решение поисковой системы о ранжировании, и оцененные Вами значения этих факторов. В таблицу обязательно включите какой-нибудь поведенческий фактор ранжирования 9.Человек последовательно вводит в поисковую систему запросы “Москва кафе и рестораны”, “Москва вузы и университеты”, “Москва плавание в бассейне” и изучает информацию по ним. Затем пользователь вводит в поисковую систему слово “стадионы”. Предложите поисковую подсказку,

	учитывающую персональные предпочтения этого пользователя. 10.Составьте текст, являющийся поисковым спамом по запросу “привет”.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-7. Алгоритмы кластеризации, классификации и ранжирования

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проводится на практическом занятии, продолжительность выполнения работы 40 минут. Студентам выдаётся несколько вариантов заданий

Краткое содержание задания:
В работе проверяется знание алгоритмов кластеризации, классификации и ранжирования;

Контрольные вопросы/задания:

Знать: алгоритмы кластеризации, классификации и ранжирования	1.Опишите байесовский классификатор 2.Опишите классификатор на базе деревьев решений 3.Опишите метод опорных векторов 4.Опишите иерархическую кластеризацию 5.Опишите многомерное шкалирование 6.Приведите пример функции активации для скрытого слоя нейросети 7.Приведите пример работы свёртки в сверточном слое нейросети 8.Приведите пример пулинга в соответствующем слое нейросети 9.Приведите пример средств, используемых для борьбы с эффектом кратковременной памяти в рекуррентных сетях 10.Приведите примеры областей, в которых применяются трансформеры

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-8. Методы распознавания частично-упорядоченных объектов и принцип конечной топологии

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проводится на практическом занятии, продолжительность выполнения работы 40 минут. Студентам выдаётся несколько вариантов заданий

Краткое содержание задания:
В работе проверяется знание методов распознавания частично-упорядоченных объектов и принципа конечной топологии

Контрольные вопросы/задания:

Знать: методы распознавания частично-упорядоченных объектов и принцип конечной топологии	1.Приведите пример тестового алгоритма распознавания 2.Опишите общую схему применения алгоритмов разделения и распознавания 3.Дайте определение конечной топологии 4.Приведите пример применения распознавания в молекулярной биологии 5.Поясните на примере обработки полиязыковых текстов важность постобработки при распознавании символов

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Для курсового проекта/работы

3 семестр

I. Описание КП/КР

Обучающемуся выдается индивидуальное задание. В рамках этого задания обучающий должен изучить материалы, разработать план программы, составить программу и отладить программу.

II. Примеры задания и темы работы

Пример задания

На вход программы подаётся изображение с графиком. На нем присутствуют основные оси координат с числовыми значениями размерности, сетка для удобства нахождения значений координат и сами линии графика. Задача программы состоит в том, чтобы распознать линии графика, получить уравнения прямых для вышеупомянутых линий, распознать координатные оси и их размерности. Для реализации программы предлагается использовать язык программирования Python и библиотеки OpenCV и Tesseract.

Тематика КП/КР:

КМ-1. Оценка выполнение раздела № 1 «Изучение материалов»
Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка 5 («отлично»), если задание получено с опозданием не более чем на 1 день

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 4 («хорошо»), если задание получено с опозданием не более чем на 2 дня

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 («удовлетворительно»), если задание получено с опозданием более чем на 3 дня

КМ-2. Оценка выполнение раздела № 2 «Разработка плана программы»
Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка 5 («отлично»), если задание получено с опозданием не более чем на 1 день

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 4 («хорошо»), если задание получено с опозданием не более чем на 2 дня

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 («удовлетворительно»), если задание получено с опозданием более чем на 3 дня

КМ-3. Оценка выполнение раздела № 3 «Составление программы»
Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка 5 («отлично»), если задание получено с опозданием не более чем на 1 день

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 4 («хорошо»), если задание получено с опозданием не более чем на 2 дня

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 («удовлетворительно»), если задание получено с опозданием более чем на 3 дня

КМ-4. Оценка выполнение раздела № 4. «Отладка программы»
Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка 5 («отлично»), если задание получено с опозданием не более чем на 1 день

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 4 («хорошо»), если задание получено с опозданием не более чем на 2 дня

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 («удовлетворительно»), если задание получено с опозданием более чем на 3 дня

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

Вопрос 1. Предварительное распределение ключей в компьютерной сети: схема Блома. Устойчивость к компрометации.
Вопрос 2. .Блочные системы шифрования: криптосистемы AES и «Кузнечик».
Вопрос 3. Семантически секретной является криптосистема
- RSA,
- Рабина,
- Эль Гамаля,
- Гольдвассер-Микали.

Процедура проведения

Экзамен проводится по билетам, содержащим два теоретических вопроса из различных разделов рабочей программы дисциплины. После ответа на вопросы билета студент должен ответить на два вопроса для проверки остаточных знаний.

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-З$_{ПК-1}$ Демонстрирует знание терминологии, основных понятий и методов решения прикладных задач

Вопросы, задания

1.Блочные системы шифрования: криптосистема DES, криптосистема ГОСТ 28147-89.
2.Блочные системы шифрования: формальное определение блочного шифра. Принципы построения. Схема Фейстеля.
3.Протоколы с нулевым разглашением секрета, допускающие неограниченные вычислительные возможности доказывающего. (Доказательство знания квадратичного вычета и знания квадратичного невычета).
4.Протоколы с нулевым разглашением секрета. Протокол Фиата – Шамира знания квадратного корня.
5.Протоколы с нулевым разглашением секрета. Доказательство знания дискретного логарифма.
6.Протоколы с нулевым разглашением секрета. Общая схема.
7.Каково назначение блоков S в сети Фейстеля
8. Перечислите общие особенности стандартов шифрования DES и ГОСТ28147-89 и специфику реализации каждого из них
9.Каковы общие режимы использования блочных шифров DES и ГОСТ28147-89 и какие режимы являются специфическими
10.В чем состоит ограничение применения режима кодовой книги (шифра простой замены)
11.Как осуществляется аутентификация с использованием блочных шифров.
12.Какой параметр блочного шифра определяется гарантированным периодом гаммы

Материалы для проверки остаточных знаний

1.Указать значение d×e mod(p-1)(q-1), где p×q=n, (e,n)-открытый ключ криптосистемы RSA, d-ее секретный ключ.

Ответы:

Это значение 1 (экспоненты зашифрования e и расшифрования d взаимно обратны по модулю функции Эйлера).

Верный ответ: Это значение 1 (экспоненты зашифрования e и расшифрования d взаимно обратны по модулю функции Эйлера).

2.Определить сообщение m_2 по его криптограмме Эль-Гамаля (C, C_{22}), если известна криптограмма Эль-Гамаля (C, C_{21}) сообщения m_1.

Ответы:

m_2=m_1 C_22(C_21)^{-1} (Вычисление возможно вследствие повторного использования рандомизатора).

Верный ответ: m_2=m_1 C_22(C_21)^{-1} (Вычисление возможно вследствие повторного использования рандомизатора).

3.Указать значение SybByte(0) функции SybByte(0) криптосистемы AES.

Ответы:

SybByte(0) =b =(1,1,0,0,0,1,1,0), поскольку элемент 0 не имеет обратного.

Верный ответ: SybByte(0) =b =(1,1,0,0,0,1,1,0), поскольку элемент 0 не имеет обратного.

4.Указать два возможных свойства односторонней функции в протоколах с нулевым разглашением, различающих их по определению значения произведения $f(x)\ f(y)$ и привести примеры таких функций.

Ответы:

Мультипликативное свойство f(x)f(y)=f(xy) (f(x)=x^2 mod n) и аддитивное свойство f(x)f(y)=f(x+y) (f(x)=f^x mod p).

Верный ответ: Мультипликативное свойство f(x)f(y)=f(xy) (f(x)=x^2 mod n) и аддитивное свойство f(x)f(y)=f(x+y) (f(x)=f^x mod p).

5.Чем отличается схема развертки ключа криптосистемы “Кузнечик” от аналогичной схемы криптосистемы AES?

Ответы:

Схема развертки ключа криптосистемы "Кузнечик" отличается применением схемы Фейстеля.

Верный ответ: Схема развертки ключа криптосистемы "Кузнечик" отличается применением схемы Фейстеля.

2. Компетенция/Индикатор: ИД-6$_{ПК-1}$ Разрабатывает и исследует алгоритмы численного решения прикладных задач

Вопросы, задания

1.Использование частичной информации при нечестной игре в покер.

2.Протокол аутентификации Шнорра.

3.Режимы использования блочных шифров. Аутентификация сообщений с использованием блочных шифров.

4.Понятие трудного предиката для односторонней функции. Пример трудного предиката для функции RSA. Алгоритм бинарного поиска с помощью оракула четности открытого текста, зашифрованного по RSA.

5.Криптосистема Эль Гамаля. Криптографическая стойкость. Атака на основе подобранного зашифрованного текста.

6.Криптосистема RSA. Алгебраические преобразования при зашифровании и расшифровании. Цифровая подпись RSA. Мультипликативное свойство криптосистемы RSA. Атака по выбираемому шифртексту.
7. Криптосистема RSA. Особенности выбора параметров при работе в компьютерной сети.
8.С использованием Алгебраического процессора составить и протестировать исполнимую спецификацию протокола Месси-Омуры.
9.С использованием Алгебраического процессора составить и протестировать исполнимую спецификацию протокола Диффи-Хелмана с атакой “человек посередине” на этот протокол.
10.С использованием Алгебраического процессора составить и протестировать исполнимую спецификацию протокола RSA с атакой по выбираемому шифр тексту.
11.С использованием Алгебраического процессора составить и протестировать исполнимую спецификацию протокола Диффи-Хелмана с аутентификацией.

Материалы для проверки остаточных знаний

1.Как смоделировать работу протокола с нулевым разглашение для доказательства его совершенства?

Ответы:

Взять произвольное допустимые значения ответа r и запроса e и вычислить значение u вызова (commit): u=f(r)(a^e)^{-1}.

Верный ответ: Взять произвольное допустимые значения ответа r и запроса e и вычислить значение u вызова (commit): u=f(r)(a^e)^{-1}.

2.Как строится атака по выбираемому шифртексту на криптосистемы, обладающие мультипликативным свойством?

Ответы:

Изменяется перехваченная криптограмма c: c'=cE_{k_з}(m'), где m' - произвольное обратимое сообщение, получают результат расшифрования D_{k_p}(c')=mm', вычисляют m=mm'm'{-1}.

Верный ответ: Изменяется перехваченная криптограмма c: c'=cE_{k_з}(m'), где m' - произвольное обратимое сообщение, получают результат расшифрования D_{k_p}(c')=mm', вычисляют m=mm'm'{-1}.

3.Какая частичная информация используется в нечестном ментальном протоколе игры в покер?

Ответы:

Символы Лежандра сообщений (карт) могут быть не одинаковыми. Если символ Лежандра некоторого сообщения отличается от символов Лежандра остальных сообщений, то и символ Лежандра второй части криптограмм будет отличаться от символов Лежандра этих частей криптограмм других сообщений. Т.о. используется информация о символах Лежандра вторых частей криптограмм.

Верный ответ: Символы Лежандра сообщений (карт) могут быть не одинаковыми. Если символ Лежандра некоторого сообщения отличается от символов Лежандра остальных сообщений, то и символ Лежандра второй части криптограмм будет отличаться от символов Лежандра этих частей криптограмм других сообщений. Т.о. используется информация о символах Лежандра вторых частей криптограмм.

4.Показать, что вскрытие протокола Шнорра равносильно решению задачи дискретного логарифмирования.

Ответы:

Используется тождество (r_1-r_2(e_1-e_2))^{-1}\equiv -s mod q, где r_1,r_2 - правильно угаданные ответы на попарно не сравнимые по модулю q вопросы.

Верный ответ: Используется тождество (r_1-r_2(e_1-e_2))^{-1}\equiv -s mod q, где r_1,r_2 - правильно угаданные ответы на попарно не сравнимые по модулю q вопросы.

3. Компетенция/Индикатор: ИД-7$_{ПК-1}$ Анализирует результаты численного и аналитического решения прикладных задач

Вопросы, задания

1.Цифровая подпись с возвратом сообщения. Электронная подпись ГОСТ Р. 34.10-2012.
2.Цифровая подпись с личностным ключом проверки.
3.Цифровая подпись Эль Гамаля. Криптографическая стойкость. Особенности использования рандомизатора и хеш-функции.
4.Криптосистема Эль Гамаля. Криптографическая стойкость и особенности выбора параметров и использования рандомизатора.
5.Распределение ключей по закрытым каналам с использованием асимметричных криптосистем: Протокол Нидмэна─Шроедера.
6.Распределение ключей по закрытым каналам с использованием симметричных криптосистем: протокол запроса-ответа с аутентификацией Нидмана-Шроедера и протокол с метками времени.
7.Предварительное распределение ключей в компьютерной сети: KDP(n,q)-схема.
8.Блочные системы шифрования: криптосистемы AES и «Кузнечик».
9.Вычислить секретный ключ криптосистемы RSA при заданных модуле n и экспоненте зашифрования e, если известна другая пара таких экспонент при том же модуле n, не прибегая к разложению модуля n.
10.Разложить модуль n криптосистемы RSA при известных экспонентах e зашифрования и расшифрования d.
11.Получить экспоненту расшифрования криптосистемы RSA методом встречи посередине.
12.Вскрыть криптосистему RSA с модулем 4757.
13.Получить сообщение m по его криптограмме Эль Гамаля (C_1,C_2), если известна криптограмма (C_1, C'_2) сообщения m'..
14.Решить проблему Диффи-Хеллмана с помощью оракула Эль Гамаля (возвращающего сообщение из крипторамы Эль гамаля).

Материалы для проверки остаточных знаний

1. Как обеспечивается максимальная длина периода в режиме обратной связи с гарантированной длиной периода?

Ответы:
Длина периода 2^{32}(2^{32}+1) обеспечивается конкатенацией последовательно вычисляемых взаимно простых элементов последовательностей, имеющих периоды 26{32} и 2^{32}-1.

Верный ответ: Длина периода 2^{32}(2^{32}+1) обеспечивается конкатенацией последовательно вычисляемых взаимно простых элементов последовательностей, имеющих периоды 26{32} и 2^{32}-1.

2.Как обеспечивается трудность дискретного логарифмирования в протоколе Шнорра?

Ответы:
При выборе системных параметров гарантируется наличие простого множителя q порядка p-1 группы F_p^*.

Верный ответ: При выборе системных параметров гарантируется наличие простого множителя q порядка p-1 группы F_p^*.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка 5 выставляется, если студент полностью ответил на оба вопроса билета и на дополнительные вопросы по билету, а также и без подготовки ответил на вопросы для проверки остаточных знаний.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 4 выставляется, если студент полностью ответил на оба вопроса билета, но затруднялся с ответами на дополнительные вопросы по билету, или была необходима подготовка к ответам на вопросы для проверки остаточных знаний.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 выставляется, если студент полностью ответил только на один вопрос билета, затруднялся с ответами на дополнительные вопросы по билету, или была необходима подготовка к ответам на вопросы для проверки остаточных знаний.

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих

3 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

Вопрос 1. Свёрточные сети
Вопрос 2. Классификатор на базе деревьев решений
Вопрос 3. Какой код правильный?
a. from tensorflow import keras
b. from numpy import keras
c. from pandas import keras
d. from sklearn import keras

Процедура проведения

Экзамен проводится в письменно-устной форме. На подготовку ответа дается 60 минут. Кроме ответа на вопросы билета, студент должен ответить на дополнительные вопросы.

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-З$_{ПК-1}$ Демонстрирует знание терминологии, основных понятий и методов решения прикладных задач

Вопросы, задания
1.Моделирование объекта. Меры сходства объектов и их совокупностей
2.Некоторые алгоритмы кластеризации

3.Решающие функции и их свойства. Распознавание линейно разделимых образов
4.Персептрон - математическая модель восприятия информации мозгом
5.Метод потенциальных функций
6.Градиентные методы построения решающих функций
7.Построение решающей функции методом минимизации среднеквадратичной ошибки
8.Байесовский классификатор для текстов и изображений
9.Классификатор на базе деревьев решений
10.Метод опорных векторов
11.Метод k ближайших соседей
12.Иерархическая кластеризация
13.Тематическое моделирование
14.Латентное размещение Дирихле
15.Неотрицательная матричная факторизация
16.Многомерное шкалирование
17.Нейронные сети с прямой связью
18. Алгоритм обратного распространения ошибки
19.Свёрточные сети
20.Рекуррентные сети
21.LSTM и GRU
22.Трансформеры
23.Предварительная обработка образов. Отбор признаков и преобразование кластеров
24.Алгоритмы разделения и распознавания
25.Применение распознавания в молекулярной биологии
26.Тестовый подход к распознаванию
27.Принцип конечной топологии
28.Распознавание оптических образов текстов

Материалы для проверки остаточных знаний

1.В распознавании образов рассматривается:

Ответы:

a. обучение без учителя, b. обучение без ученика, c. обучение без учебников, d. обучение без училища.

Верный ответ: a. обучение без учителя

2.Персептрон представляет собой:

Ответы:

a. опорный вектор, b. метрику, c. нейронную сеть, d. метод потенциалов.

Верный ответ: c. нейронную сеть

3.Алгоритмом кластеризации не является:

Ответы:

a. пороговый алгоритм, b. алгоритм Евклида, c. алгоритм максимального расстояния, d. алгоритм k средних.

Верный ответ: b. алгоритм Евклида,

4.Разделяющая поверхность не может быть:

Ответы:

a. сферой, b. континуум-гипотезой, c. плоскостью, d. гиперболоидом.

Верный ответ: b. континуум-гипотезой,

5.В нейронной сети знание веса и смещения каждого нейрона является самым важным. Если вы можете каким-то образом получить правильное значение веса и смещения для каждого нейрона, вы можете аппроксимировать любую функцию. Какой лучший способ подойти к этому?

Ответы:

a. Назначьте случайные значения и молитесь Богу, чтобы они были правильными b. Поиск всех возможных комбинаций весов и смещений, пока Вы не получите лучшее значение c. Итеративно проверить после присвоения значений, насколько далеко Вы находитесь от лучших значений, и немного изменить присвоенные значения, чтобы сделать их лучше d. Ни один из вышеперечисленных

Верный ответ: c. Итеративно проверить после присвоения значений, насколько далеко Вы находитесь от лучших значений, и немного изменить присвоенные значения, чтобы сделать их лучше

6.Какие два типа нейросетей здесь?

Ответы:

a. Биологические нейронные сети и искусственные нейронные сети b. Геологические нейронные сети и искусственные нейронные сети c. Химические нейронные сети и биологические нейронные сети d. Химические нейронные сети и геологические нейронные сети

Верный ответ: a. Биологические нейронные сети и искусственные нейронные сети

7.При использовании алгоритма обратного распространения ошибки:

Ответы:

a. нейронная сеть сходится, когда ошибка проверки остается низкой, а примеры обучения не вызывают значительных изменений в весах сети. b. нейронная сеть сходится, когда ошибка проверки остается высокой, а примеры обучения не вызывают значительных изменений в весах сети. c. нейронная сеть сходится, когда ошибка проверки остается низкой, а примеры обучения вызывают значительные изменения в весах сети.

Верный ответ: a. нейронная сеть сходится, когда ошибка проверки остается низкой, а примеры обучения не вызывают значительных изменений в весах сети.

8.Для алгоритма обратного распространения нам нужна:

Ответы:

a. дифференцируемая функция, b. не дифференцируемая функция, c. мы можем использовать любую функцию.

Верный ответ: a. дифференцируемая функция,

9.Процессом обучения нейронной сети называют:

Ответы:

a. процесс подстройки весовых коэффициентов сети b. процесс подбора входных данных c. процесс подбора архитектуры сети d. процесс подстройки количества скрытых слоев

Верный ответ: a. процесс подстройки весовых коэффициентов сети

10.Нейроны складываются вместе, образуя сеть, которая может быть использована для аппроксимации любой функции. Когда модель нейронной сети становится моделью глубокого обучения?

Ответы:

a. Когда Вы добавляете больше скрытых слоев и увеличиваете глубину нейронной сети b. Когда существует более высокая размерность данных c. Когда проблема заключается в проблеме распознавания изображений d. Ни один из них

Верный ответ: a. Когда Вы добавляете больше скрытых слоев и увеличиваете глубину нейронной сети

11.Алгоритм обучения персептрона

Ответы:

a. всегда сходится b. всегда расходится c. сходимся, только если задача линейно разделима

Верный ответ: c. сходимся, только если задача линейно разделима

12.Какой из следующих методов относится к обучению без учителя

Ответы:

a. байесовский классификатор b. кластеризация методом k средних c. метод k ближайших соседей d. метод опорных векторов

Верный ответ: b. кластеризация методом k средних

2. Компетенция/Индикатор: ИД-5$_{ПК-1}$ Применяет современные методы исследования математических моделей

Вопросы, задания

1.Библиотека TensorFlow
2.Библиотека Keras
3.Библиотека Numpy
4.Библиотека Scikit-Learn
5.Библиотека PyTorch
6.Библиотека Matplotlib
7.Библиотека Pandas
8.Библиотека Natural Language Toolkit
9.Библиотека DeepPavlov
10.Библиотека Natasha
11.Методы создания поисковых систем
12.Библиотека tesseract
13.Библиотека OpenCV
14.Запишите команду, добавляющую в модель нейронной сети, составленную с помощью библиотеки keras, полносвязный слой с размерностью выходного пространства 10 и функцией активации softmax
15.Запишите команду для прогноза значения переменной y_model по экспериментальным данным, представленным переменной Xtest, использующую уже обученную на данных обучающей выборки модель model, созданную с помощью библиотеки scikit-learn
16.Запишите команду для подключения модуля nn из библиотеки PyTorch
17.Составьте таблицу, по вертикали которой будут выписаны 3 первых сайта из выдачи поисковой системы по запросу “сложение матриц”, а по горизонтали факторы ранжирования, которые Вы считаете повлиявшими на решение поисковой системы о ранжировании, и оцененные Вами значения этих факторов. В таблицу обязательно включите какой-нибудь поведенческий фактор ранжирования
18.Человек последовательно вводит в поисковую систему запросы “Москва кафе и рестораны”, “Москва вузы и университеты”, “Москва плавание в бассейне” и изучает информацию по ним. Затем пользователь вводит в поисковую систему слово “стадионы”. Предложите поисковую подсказку, учитывающую персональные предпочтения этого пользователя.
19.Составьте текст, являющийся поисковым спамом по запросу “привет”.

Материалы для проверки остаточных знаний

1.Какой код правильный?

Ответы:

a. from tensorflow import keras b. from numpy import keras c. from pandas import keras d. from sklearn import keras

Верный ответ: a. from tensorflow import keras

2.Какой код правильный?

Ответы:

a. from numpy.naive_bayes import GaussianNB b. from pandas.naive_bayes import GaussianNB c. from sklearn.naive_bayes import GaussianNB d. from torch.naive_bayes import GaussianNB

Верный ответ: c. from sklearn.naive_bayes import GaussianNB

3.Какой код правильный?

Ответы:

a. import numpy.nn as nn b. import pandas.nn as nn c. import scipy.nn as nn d. import torch.nn as nn

Верный ответ: d. import torch.nn as nn

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. На вопросы углубленного уровня даны неверные ответы

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих

Для курсового проекта/работы:

3 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты КП/КР

На защите курсовой работы обучающемуся задаются теоретические и практические вопросы по представленной расчетно-пояснительной записке.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

III. Правила выставления итоговой оценки по курсу

Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»