Приложение к рабочей программе дисциплины (практики)

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН)

Факультет искусственного интеллекта

(наименование основного учебного подразделения)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

ДИСКРЕТНАЯ МАТЕМАТИКА

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

Освоение дисциплины (практики) ведется в рамках реализации основной профессиональной образовательной программы (ОП ВО, профиль/ специализация):

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(направленность (профиль) ОП ВО)

Москва, 2025

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

1. Виды контроля по периодам обучения

1.1.Материалы для проведения текущего контроля:

Перечень вопросов для контрольных работ:

КОНТРОЛЬНАЯ РАБОТА 1

1. Бинарные отношения элементов множества
2. Отображения множеств
3. Формула включений-исключений
4. Перестановки, размещенич и сочетания
5. Правило произведения. Размещения и перестановки с повторениями
6. Количество подмножеств данного конечного множества
7. Мультимножества. Сочетания с повторениями
8. Числа Стирлинга первого рода.
9. Числа Стирлинга второго рода.
10. Числа Белла.

КОНТРОЛЬНАЯ РАБОТА 2

1. Построение конечных колец и полей классов вычетов
2. Функции и уравнения в конечных кольцах и полях
3. Сравнения по модулю с неизвестными
4. Методы решения сравнений по модулю
5. Односторонние функции
6. Дискретный логарифм
7. Применение конечных односторонних функций в современной криптографии
8. Обмен ключами Диффи-Хеллмана
9. Асимметричный шифр RSA
10. Алгоритм Евклида
11. Уравнения шифрования RSA

КОНТРОЛЬНАЯ РАБОТА 3

1. Линейные пространства над конечными полями
2. Расстояние Хэмминга
3. Норма Хэмминга
4. Понятие блоковых кодов и их корректирующие свойства
5. Кодовое расстояние
6. Способности кода к исправлению искажений
7. Линейные блоковые коды
8. Процессы кодирования и декодирования
9. Коды Хэмминга

2. Сборником типовых практических задач для контрольных работ:

Сколькими способами можно расположить 8 ладей на шахматной доске 8х8 так, чтобы они не могли бить друг друга?

Сколькими способами можно посадить п гостей за круглым столом, если способы посадки, отличающиеся сдвигом по кругу, считать одинаковыми?

Сколько существует перестановок п элементного множества, в которых данные т элементов:

Сколькими способами можно посадить за круглым столом п мужчин и п женщин так, чтобы никакие два лица одного пола не сидели рядом, если способы посадки, отличающиеся сдвигом по кругу, не считаются одинаковыми?

Сколькими способами 7 книг разных авторов можно расставить на полке в один ряд?

Сколькими способами можно разложить 8 различных писем в 8 различных конвертов, если в каждый конверт кладётся только одно письмо?

Сколькими способами можно выбрать 3- х делегатов на конференцию из группы в 25 человек?

У одного человека 11 различных марок для обмена, а у другого 15, причём одинаковых марок у них нет. Сколькими способами они могут организовать обмен 3 марок?

В турнире принимали участие п шахматистов и каждые два шахматиста встретились 1 раз. Сколько партий было сыграно в турнире?

Сколько существует кортежей из 0 и 1 длины п содержащих к единиц?

На плоскости даны п точек никакие три из которых не лежат на одной прямой. Сколько различных прямых можно провести через эти точки?

Сколькими способами читатель может выбрать две книги из пяти различных книг?

Сколькими способами из 10 человек, играющих в городки, можно составить команду из 4 человек?

В розыгрыше первенства по волейболу принимают участие команды 6 факультетов, при этом любые две команды играют между собой только один матч. Сколько всего запланировано календарных игр?

У Нины есть 8 различных книг по математике, а у Славы - 10 различных книг по физике. Сколькими способами они могут обменять друг с другом по 6 книг?

Из 2- х математиков и 10- экономистов надо составить комиссию в составе 7- ми человек. Сколькими способами может быть составлена комиссия, если в неё должен входить хотя бы один математик?

Сколькими способами можно разместить 30 различных предметов по 6 ящикам чтобы в каждом ящике оказалось по 5 предметов?

Найти число 5 буквенных «слов», образованных буквами «а, б, в» и в которых буква «а» появляется самое большее 2 раза, буква «б» - 1 раз, буква «в» - 3 раза.

Сколько пятизначных чисел можно составить из цифр числа 75266522?

Сколькими способами можно расположить в один ряд 3 зелёные и 4 красные лампочки?

Сколькими способами группу в 10 человек можно разбить на 3 подгруппы, по 2,3,5 человека в подгруппе, для работы в библиотеке, спортзале и столовой, соответственно?

Сколькими способами можно распределить 7 молодых специалистов по трём школам, которым, соответственно, нужны 1,2,4 учителя?

Десять человек разбиты на 5 групп, по два человека в каждой. Сколькими способами это можно сделать?

Сколько можно составить различных костей домино, если использовать для их образования все цифры? только три цифры?

Сколько существует треугольников, длины сторон которых принимают одно из следующих значений 4,5,6,7? 7,8,9,10?

Трое ребят собрали 40 яблок. Сколькими способами они могут их разделить?

Найти число различных последовательностей букв, которое можно получить, переставляя буквы слова "математика".

2.2 Материалы для проведения промежуточной аттестации:

Вид промежуточной аттестации – зачет с оценкой.
Форма проведения - устный опрос.
Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию:
Перечень тем и вопросов, выносимых на промежуточную аттестацию:

Тема 1. Комбинаторика конечных множеств
Количество подмножеств конечного множества
Мощность множества. Кардинальные числа
Операции над множествами
Декартово произведение множеств
Сюръективные, инъективные, биективные отображения множеств
Композиция отображений
Формула включений - исключений
Комбинаторное правило умножения
Кортежи и размещения с повторениями
Биномиальная схема. Бином Ньютона
Треугольник Паскаля
Элементы комбинаторики
Перестановки, размещения, сочетания
Размещения с повторениями
Сочетания с повторениями
Перестановки с повторениями
Основные комбинаторные схемы

Тема 2. Подстановки и их свойства. Мультимножества
Основные алгебраические структуры: Полугруппы, Группы, Кольца, Поля
Группа подстановок
Циклическое представление подстановок
Четность подстановок
Бинарные отношения элементов множества
Отображения множеств
Формула включений-исключений
Перестановки, размещенич и сочетания
Правило произведения. Размещения и перестановки с повторениями
Количество подмножеств данного конечного множества
Мультимножества. Сочетания с повторениями
Числа Стирлинга первого рода.
Числа Стирлинга второго рода.
Числа Белла.

Тема 3. Функции и уравнения в конечных кольцах и полях
Построение конечных колец и полей классов вычетов
Функции и уравнения в конечных кольцах и полях
Сравнения по модулю с неизвестными
Методы решения сравнений по модулю
Односторонние функции
Дискретный логарифм
Задачи факторизации

Тема 4. Применение конечных односторонних функций в современной криптографии

Применение конечных односторонних функций в современной криптографии
Обмен ключами Диффи-Хеллмана
Протоколы распределения ключей
Асимметричный шифр RSA
Алгоритм Евклида
Нахождение открытых и секретных ключей
Уравнения шифрования RSA

Тема 5. Линейные пространства над конечными полями

Построение конечных колец
Построение конечных полей
Кольца и поля вычетов по модулю
Линейная зависимость векторов.
Базисы и размерность линейного пространства.
Подпространства линейных пространств.
Факторпространства.
Скалярное произведение в конечном пространстве
Расстояние в конечном пространстве над конечным полем
Расстояние Хэмминга
Норма Хэмминга

Тема 6. Блоковые коды и их корректирующие свойства

Понятие блоковых кодов и их корректирующие свойства
Кодовое расстояние
Способности кода к исправлению искажений
Линейные блоковые коды
Процессы кодирования и декодирования
Коды Хэмминга

Перечень задач, выносимых на промежуточную аттестацию:

Используя алгоритм Диффи-Хеллмана по заданным значениям p=61 , m=5, x=7, y=11, вычислить значение общего ключа.
Открытый ключ системы RSA задается числами n=33 , e=7. Используя этот ключ было получено шифрованное сообщение {9; 1; 29}. Найти исходное открытое сообщение {M_1; M_2; M_3}.

Подсчитайте количество различных последовательностей букв, которые могут быть получены всевозможными перестановками букв каждого из приведенных слов.

a) хор;
b)мама;
c) рама;
d) огого;
e)около.

Три провайдера обеспечивают доступ в Интернет 11 различным пользователям. Сколькими различными способами может быть осуществлено распределение пользователей по провайдерам, при условии что услугами 1го, 2го и 3го провайдера пользуются соответственно 6, 3 и 2 пользователя?

Сколько различных ситуаций возможно, когда в 10-ти этажном здании из 13 пассажиров лифта на трех этажах выйдут по одному человеку, на двух – по два и на двух - по три человека?

Сколько различных частных производных 10 порядка имеет всюду дифференцируемая функция четырех аргументов?

В кондитерском магазине продаются 4 сорта пирожных: наполеоны, эклеры, песочные и слоеные. Сколькими способами можно купить 10 пирожных?

Дана подстановка $\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 8\,6\,4\,7\,5\,3\,2\,1 \end{pmatrix}$

Записать подстановку в виде произведения независимых циклов

Записать подстановку в виде произведения транспозиций

Определить четность подстановки

Решить уравнение: $729x \equiv 33 \pmod{321}$

Решить уравнение: $125x \equiv 243 \pmod{119}$

В турнире принимали участие п шахматистов и каждые два шахматиста встретились 1 раз. Сколько партий было сыграно в турнире?

Сколько существует кортежей из 0 и 1 длины п содержащих к единиц?

На плоскости даны п точек никакие три из которых не лежат на одной прямой. Сколько различных прямых можно провести через эти точки?

Сколькими способами читатель может выбрать две книги из пяти различных книг?

Сколькими способами из 10 человек, играющих в городки, можно составить команду из 4 человек?

В розыгрыше первенства по волейболу принимают участие команды 6 факультетов, при этом любые две команды играют между собой только один матч. Сколько всего запланировано календарных игр?

У Нины есть 8 различных книг по математике, а у Славы - 10 различных книг по физике. Сколькими способами они могут обменять друг с другом по 6 книг?

Из 2- х математиков и 10- экономистов надо составить комиссию в составе 7- ми человек. Сколькими способами может быть составлена комиссия, если в неё должен входить хотя бы один математик?

2. Критерии и показатели оценивания результатов обучения

а. Планируемые результаты обучения по дисциплине

Таблица № 1

Результаты освоения образовательной программы *(Код и формулировка компетенций)*	**Уровень освоения компетенции**	**Перечень планируемых результатов обучения по дисциплине** *(в целях формирования названной компетенции)*
ОК-8 способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления	Базовый уровень	**Знать:** основные принципы построения современной дискретной математики. **Уметь:** применять методы дискретного анализа и моделирования. **Владеть:** принципами математической логики.
ОК-9 способностью логически верно, аргументированно и	Базовый уровень	**Знать:** основные принципы логического вывода. **Уметь:** корректно использовать основные понятия, связанные с дискретной математической проблематикой.

ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии		**Владеть:** основными методами математического доказательства**.**
ОК-11 способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства	Базовый уровень	**Знать:** основные законы научного познания. **Уметь:** осуществлять поиск необходимой информации и применять ее для решения стоящей практической задачи; доказательно обосновать выбор тех или иных средств и методов для решения конкретной задачи. **Владеть:** аксиоматическим подходом к приобретению новых знаний.
ПК-1 способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности	Базовый уровень	**Знать:** теоретические основы изученных разделов дискретной математики; основные понятия и методы дискретного анализа; основные понятия и методы комбинаторики, а также конечных полей и дискретного кодирования; проявлять высокую степень их понимания. **Уметь:** применять теоретические знания к конкретным практическим задачам; формулировать на математическом языке проблемы, поставленные в терминах других предметных областей; составлять математические модели типовых профессиональных задач и находить способы их решений; интерпретировать профессиональный (физический) смысл полученного математического результата; применять типовые аналитические и численные методы решения поставленных профессиональных задач. **Владеть:** профессиональной терминологией, принятой в дискретной математике; математической логикой, необходимой для формирования суждений по соответствующим профессиональным и научным проблемам; владеть методами анализа и синтеза изучаемых явлений и процессов. Владеть навыками работы с моделями шифров, текстов и псевдослучайных последовательностей
ПК-30 способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности	Базовый уровень	**Знать:** математические принципы построения криптографических алгоритмов; основные приемы математического синтеза шифров; особенности использования математического моделирования в криптографии **Уметь:** применять дискретные методы при решения конкретных задач; строить математические модели, отражающие наиболее существенные стороны современных систем защиты информации; использовать математические методы анализа систем защиты информации; проводить статистический анализ стойкости шифров; применять математические методы для выявления слабостей конкретных систем шифрования **Владеть:** навыками использования математических компьютерных программ, позволяющих выполнять громоздкие математические вычисления на ЭВМ; использовать возможности компьютерной техники для качественного исследования существенных свойств конкретных систем защиты информации.

b. Критерии и показатели оценки

Таблица № 2

Критерии	Оценка			
	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»
1.Знание теоретических основ дискретной математики.	Студент демонстрирует глубокое знание теоретических основ и принципов, базовых понятий и определений, которые используются в	Студент достаточно хорошо владеет знаниями теоретических основ и принципов, базовых понятий и определений дискретной математики.	Студент затрудняется с изложением теории, поверхностно ориентируется в базовых понятиях и определениях дискретной математики.	Студент не понимает поставленной проблемы, не знает теоретических основ и принципов дискретной математики.
2. Умение применять теоретические знания к конкретным практическим заданам	Студент уверенно применяет теоретические положения дискретной математики к решению задач	Студент испытывает затруднения при применении теоретических положений дискретной математики к решению задач.	Студент может применить теоретические положения к решению задач только после наводящих вопросов, допуская	Студент не умеет применять теоретические положения к практическим задачам.
3. Владение профессиональной терминологией, принятой в дискретной математике.	Студент демон-стрирует свобод-ное владение понятийным ап-паратом и умение быть корректным в употреблении математической терминологией.	Студент достаточно хорошо владеет профессиональной терминологией, в случае ошибки в употреблении термина способен исправить ее сам.	Студент слабо владеет профес-сиональной тер-минологией, до-пускает неточ-ности в интер-претации понятий и определений в данной предмет-ной области.	Студент не вла-деет профессио-нальной терми-нологией и не разбирается в понятийном ап-парате мате-матики.

с. Порядок выставления общей оценки в рамках зачета с оценкой.

Итоговая аттестация предусмотрена в форме зачета с оценкой, который проводится в виде устного собеседования по контрольным вопросам. Экзаменуемому предлагается два теоретических вопроса и одна задача. Вклад в общую оценку теоретических вопросов и практической задачи составляет 50% на 50%.

Важнейшими критериями оценки знаний и умений обучаемых по теоретическим вопросам являются:

– степень усвоения учебной программы;

– содержание ответа на контрольные вопросы: логичность и доказательность изложения;

– степень творчества и самостоятельности в раскрытии поставленных вопросов.

Важнейшими критериями оценки выполнения практического задания является:

– умение применить теоретические знания при решении задач;

– степень самостоятельности и оригинальности решения практической задачи.