# *Программа вступительного экзамена по направлению 1.2. Компьютерные науки и информатика*

**Целью** вступительного испытания является оценка уровня освоения поступающим компетенций, необходимых для обучения по направлению ***1.2. «Компьютерные науки и информатика»***по программам подготовки научных и научно-педагогических кадров в аспирантуре.

**Программы вступительных испытаний при приеме на обучение в аспирантуре формируются** на основе требований Национального исследовательского Университета ИТМО. Экзамен проводится по билетам. Билет содержит 2 вопроса в соответствии с программой, а также вопрос о планируемом диссертационном исследовании абитуриента.

**Форма вступительного испытания:** устно-письменная

**Форма вступительного испытания с использованием дистанционных технологий:** тест, устно-письменная

**Продолжительность** проведения вступительного испытания. Продолжительность вступительного испытания - не более 90 минут.

**Критерии оценивания:** “неудовлетворительно”, “Удовлетворительно”, “Хорошо”, “Отлично”

**Минимальный проходной балл,** подтверждающий успешное прохождение вступительных испытаний: оценка “удовлетворительно”.

**Перечень принадлежностей**, которые поступающий имеет право пронести в аудиторию во время проведения вступительного испытания: письменные принадлежности, непрограммируемый калькулятор.

**Научная специальность 1.2.1. «Искусственный интеллект и машинное обучение»**

1. Линейные пространства векторов. Скалярное произведение. Понятие базиса и линейной независимости элементов линейного пространства. Преобразования базиса.

2. Определение матрицы. Операции с матрицами (умножение на скаляр, сложение, умножение матриц, транспонирование матриц). Обратная матрица и методы ее получения. Функции от матриц.

3. Собственные числа матрицы и методы их получения. Характеристический полином. Свойства собственных чисел и собственных векторов для специфических видов матриц (симметричные, положительно-определенные). Понятие обусловленности и его характеристики.

4. Производные. Необходимое и достаточное условие дифференцируемости функции. Частные производные. Полный дифференциал. Производная и дифференциал сложной функции.

5. Градиент функции. Производные по направлению. Необходимые и достаточные условия экстремума функции многих переменных. Условные экстремумы. Метод множителей Лагранжа.

6. Неопределенный и определенный интеграл, и методы их вычисления. Теорема о среднем и ее практический смысл. Виды многомерных интегралов (по объему, по поверхности, и пр.). Теорема Гаусса-Остроградского.

7. Задачи аппроксимации функций (интерполяция, экстраполяция, приближение в среднем). Способы построения интерполяционного полинома. Аппроксимации на основе ортогональных базисов. Понятие сплайна.

8. Численные методы оптимизации: методы Ньютона и секущей, методы покоординатного и градиентного спуска. Улучшение сходимости градиентных методов.

9. Численные методы оптимизации, основанные на случайных числах. Метод Монте-Карло, линейный случайный поиск, метод оптимизации отжигом.

10. Прямые и итерационные методы решения систем линейных алгебраических уравнений. Методы для систем с матрицами специального вида (ленточные, треугольные, положительно-определенные).

11. Линейные пространства функций (примеры). Скалярное произведение и норма. Операторы над линейными пространствами функций. Функционалы. Собственные числа и функции оператора в пространстве L2.

12. Определение вероятности. Вероятностная модель и вероятностное пространство. Вероятность случайного события и методы ее статистического оценивания по выборке.

13. Модель случайной величины. Закон, функция, плотность распределения. Квантили и моменты распределений, методы их статистического оценивания по выборке.

14. Вероятностные и толерантные интервалы: сходства и различия. Понятия точечного и интервального оценивания. Доверительные интервалы. Несмещенные и эффективные оценки

15. Параметрическое оценивание распределений случайной величины. Метод моментов. Метод наибольшего правдоподобия и его численная реализация. Способы проверки качества параметрического оценивания.

16. Статистические гипотезы и статистические критерии. Односторонние и двусторонние критерии. Критерии согласия. Параметрические критерии. Ошибки первого и второго рода. Мощность критерия.

17. Модель многомерной случайной величины. Совместные и условные распределения. Условные моменты распределений и их оценивание по выборке. Многомерное распределение Гаусса и его свойства.

18. Случайные процессы и временные ряды. Понятие стационарности. Ковариационная (корреляционная функция). Теорема Карунена-Лоэва. Спектральная плотность случайных процессов.

19. Графы. Основные понятия: ориентированность графа, степени вершины, связность, цепи и циклы (Эйлеров, Гамильтонов). Подграфы и клики. Способы представления графа: матрицы и списки инцидентности и смежности. Важные частные случаи: деревья, направленные ациклические графы, двудольные графы.

20. Алгоритмы на графах. Алгоритмы обхода (поиска на) графах. Обнаружение кратчайшего пути и минимального цикла в графе. Построение остовного дерева.

21. Основные понятия машинного обучения. Отличие машинного обучения от статистики. Методы на обучении с учителем. Методы на обучении без учителя. Метрики качества алгоритмов машинного обучения.

22. Цикл обучения. Понятия обучающей и тестовой выборки. Отложенная выборка. Кросс-валидация. Понятия недообучения и переобучения. Дилемма смещения и разброса. Размерность Вапника-Червоненкиса.

24. Понятия классификации и кластеризации. Метрические, иерархические, вероятностные методы классификации и кластеризации. DBSCAN и kNN Оценка качества классификации и кластеризации. Средства реализации в высокоуровневых языках программирования.

25. Понятие регрессии. Типы регрессии. Методы численного решения задач регрессии. Способы задания целевой функции в задаче регрессии. Метод наименьших квадратов. Методы машинного обучения для решения задач регрессии. Средства реализации в высокоуровневых языках программирования.

26. Понятие искусственной нейронной сети. Типы нейронных сетей. Понятие стохастического градиента для обучения нейронной сети. Многослойный перцептрон. Сверточные нейронные сети. Средства реализации в высокоуровневых языках программирования.

27. Методы снижения размерности данных. Метод главных компонент. Метод канонических корреляций. Методы факторного анализа. Нелинейные методы снижения размерности. Средства реализации в высокоуровневых языках программирования.

28. Принцип повышения размерности пространства. Метод опорных векторов. Понятие и свойства ядра. Метод Kernel-Trick. Средства реализации в высокоуровневых языках программирования.

29. Построение списка решений и дерева решений. Редукция деревьев решений. Понятие бэггинга и бустинга для деревьев решений. Случайный лес и способы его построения. Средства реализации в высокоуровневых языках программирования.

30. Обучение с подкреплением. Модели агентов и отклика среды. Задачи, решаемые обучением с подкреплением. Средства реализации в высокоуровневых языках программирования.

31. Ассоциативный анализ и задача о "покупательской корзине". Алгоритмы аprior и FP-Growth. Средства реализации в высокоуровневых языках программирования.

32. Способы представления знаний. Модели графов знаний. Полнота графов знаний. Методы прямого и обратного вывода по графам знаний. Онтологическая модель и средства ее реализации.

33. Экспертные методы в принятии решений. Принятие решений при многих критериях. Множество Парето. Экспертные системы поддержки принятия решений.

34. Методы машинного обучения для анализа текстовой информации. Понятие эмбеддинга. Методы построения и использования эмбеддингов при работе с текстом. Средства реализации в высокоуровневых языках программирования.

35. Графовые вероятностные модели. Методы структурного обучения и обучения распределений в узлах графовых вероятностных моделей. Типы графовых вероятностных моделей. Меры качества и целевые функции, применяемые при обучении графовых вероятностных моделей. Средства реализации в высокоуровневых языках программирования.

36. Генеративные методы машинного обучения. Генеративно-состязательные сети. Вариационные автокодировщики. Байесовские сети. Принципы работы, оценка качества. Средства реализации в высокоуровневых языках программирования.

# Научная специальность 1.2.2. «Математическое моделирование, численные методы и комплексы программ»

1. Основные принципы математического моделирования. Виды математических моделей. Области применения.
2. Компьютерное и имитационное моделирование. Методология имитационного моделирования.
3. Компьютерные среды и языки имитационного моделирования.
4. Линейная алгебра и системы линейных алгебраических уравнений.
5. Методы решения систем линейных алгебраических уравнений.
6. Линейные операторы. Матричные разложения.
7. Линейные обыкновенные дифференциальные уравнения и системы.
8. Математическое программирование. Типы экстремумов функций многих переменных, условия локального экстремума, метод множителей Лагранжа.
9. Задачи линейного программирования. Основные принципы симплекс-метода.
10. Случайные величины. Распределение дискретных случайных величин. Характеристики распределений.
11. Основные законы распределения непрерывных случайных величин.
12. Генеральная совокупность. Статистическая выборка. Репрезентативность выборки.
13. Точечные и интервальные оценки математического ожидания и дисперсии.
14. Закон больших чисел. Центральная предельная теорема.
15. Понятие статистической гипотезы и статистического критерия. Основные понятия теории статистических оценок и свойства оценок.
16. Случайные процессы, основные понятия, их классификация. Конечные цепи Маркова.
17. Понятие системы массового обслуживания. Системы массового обслуживания с отказами. Системы массового обслуживания без отказов.
18. Поток заявок в системах массового обслуживания. Простейший поток. Поток с переменным параметром. Стационарные потоки.
19. Марковский поток. Уравнения Эрланга. Процесс типа «гибель и размножение».
20. Комбинаторные методы дискретного анализа. Классические задачи комбинаторного анализа. Разбиения и размещения.
21. Элементарная теория множеств. Булева алгебра. Логика высказываний. Построение ДНФ и КНФ логической функции.
22. Логика предикатов первого порядка. Теорема о дедукции. Теорема о полноте. Методы логического вывода.
23. Бинарные отношения и графы. Способы представления графов.
24. Пути в графе. Нахождение кратчайших путей в ориентированном графе.
25. Классификация задач принятия решений. Этапы принятия решений. Системы поддержки принятия решений.
26. Функция выбора в задачах принятия решений. Понятия наследуемости и независимости. Теория полезности.
27. Экспертные методы в принятии решений. Принятие решений при многих критериях. Множество Парето.
28. Подходы к проектированию алгоритмов: «разделяй и властвуй», динамическое программирование, жадная стратегия.
29. Алгоритмы сортировки, двоичного поиска.
30. Алгоритмы на графах: обход графа, поиск кратчайших путей, построение минимального остовного дерева.
31. Применение машинного обучения для моделирования объектов.
32. Обучение с учителем, обучение без учителя и обучение с подкреплением.
33. Проблема сепарабельности задач. Методы распределенного моделирования.
34. Методы организации вычислительного эксперимента.
35. Методы оценки адекватности математических моделей объектов на основе натурного эксперимента.
36. Методы компьютерного имитационного моделирования.
37. Проблема генерации случайных чисел для имитационного моделирования.

# Научная специальность 1.2.3. «Теоретическая информатика, кибернетика» (физ-мат.)

1. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события.
2. Условная вероятность. Формула полной вероятности. Теорема Байеса.
3. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
4. Дискретные и непрерывные случайные величины. Биноминальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова.
5. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
6. Основы теории чисел. Понятие группы, кольца, поля. Арифметика в конечных полях.
7. Китайская теорема об остатках. Расширенный алгоритм Евклида. Теорема Лагранжа о порядке подгрупп конечной группы.
8. Классификация случайных процессов. Марковские случайные процессы и их свойства.
9. Основные свойства информации. Мера количества информации. Энтропия. Взаимная информация.
10. Прямая и обратная теоремы кодирования источников. Неравенство Крафта. Код Хаффмана.
11. Прямая и обратная теоремы канального кодирования. Неравенство Фано.
12. Канальное кодирование. Линейные блоковые коды и их параметры. Границы Хемминга и Варшамова-Гилберта.
13. Циклические коды. Коды БЧХ. Ключевое уравнение декодирования кодов БЧХ и методы его решения.
14. Коды с малой плотностью проверок на четность и их декодирование.
15. Методы математической теории языков и грамматик.
16. Основные понятия теории конечных автоматов и теории графов.
17. Понятие сложности алгоритмов. Классы P и NP. Полиномиальная сводимость задач.
18. Методы многомерной оптимизации.
19. Показатели надежности. Классификация отказов. Понятие избыточности и ее классификация. Понятие резервирования. Восстанавливаемые и невосстанавливаемые системы и их классификация. Показатели надежности восстанавливаемых и невосстанавливаемых систем.
20. Методы повышения надежности и резервирование. Виды резервирования. Структурное резервирование. Функциональное резервирование. Временное резервирование. Информационное резервирование. Алгоритмическое резервирование.
21. Базовые и сетевые модели передачи информации в компьютерных сетях.
22. Анализ свойств и задачи оптимизации процессов обработки информации в вычислительных системах и комплексах.
23. Аналитические и статистические методы исследования характеристик процессов.
24. Методы и средства кодирования информации в виде данных. Проектирование моделей̆ данных.
25. Системы управления базами данных. Языки манипулирования данными, языки запросов.
26. Семантические сети. Фреймы - системно-структурное описание предметной области. Продукционные системы представления знаний. Канонические системы Поста. Редукционные системы.
27. Классификационные системы: иерархические классификации, фасетные классификации, алфавитно-предметные классификации. Тезаурусные методы представления знаний.
28. Основные методы распознавания образов.
29. Предварительная обработка данных в задачах анализа: нормализация, стандартизация, обработка пропущенных значений. Способы получения репрезентативных выборок.
30. Задачи классификации: общая постановка, виды, обзор методов решения, возможные приложения.
31. Языки и модели человеко-машинного взаимодействия.
32. Методы и модели распознавания и понимания речи.
33. Методы синтеза речи и изображений.
34. Методы и алгоритмы анализа текста, извлечения данных из текстов на естественном языке. Тематическое моделирование.
35. Методы и алгоритмы фильтрации и распознавания изображений.
36. Понятие и свойства искусственного интеллекта.
37. Понятие и свойства искусственной когнитивной системы.
38. Основные понятия и виды информационного поиска.
39. Модели оценки надежности и оптимизация распределенных вычислительных систем.
40. Знаковые системы. Семиотический треугольник и его элементы. Понятия «экстенсионал» и «интенсионал».
41. Основные понятия эволюционного моделирования и генетические алгоритмы
42. Нейросетевые методы классификации и регрессии. Многослойные нейронные сети.

# Научная специальность 1.2.4. «Кибербезопасность»

1. Информация, сообщение, информационные системы и процессы как объекты информационной безопасности. Основные свойства информации. Мера количества информации. Энтропия. Модели стоимости информации.
2. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события.
3. Условная вероятность. Формула полной вероятности. Теорема Байеса.
4. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
5. Дискретные и непрерывные случайные величины. Биноминальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова.
6. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
7. Основы теории чисел. Понятие группы, кольца, поля.
8. Криптографические методы зашиты информации. Основные постулаты криптографии. Исторические шифры.
9. Криптоаналитика. Теоретическая, практическая и временная стойкость системы криптографической защиты. Современные поточные и блочные алгоритмы шифрования.
10. Системы симметричного шифрования. Вопросы генерации и распределения ключей.
11. Обоснование надежности криптографической защиты.
12. Системы асимметричного шифрования, открытый ключ, электронная подпись. Атака «человек посредине».
13. Псевдослучайные последовательности: области применения в задачах обеспечения информационной безопасности; методы получения; способы оценки качества.
14. Современная криптография с открытым ключом: основные идеи, концепция. Криптосистемы RSA, El Gamal, рюкзака.
15. Электронная цифровая подпись: основные идеи, концепции, Подпись RSA, El Gamal. Отрицаемая и неотрицаемая подпись.
16. Криптографические протоколы. Протоколы аутентификации без разглашением, протокол подбрасывания монетки.
17. Математический аппарат для криптографии: китайская теорема об остатках, расширенный алгоритм Евклида, арифметика в конечных полях.
18. Эллиптические кривые в криптографии. Основные концепции и идеи. Криптосистема ElGamal, протокол Месси-Омура.
19. Пороговые схемы разделения секрета на Китайской теореме об остатках, интерполяционной формуле Лагранжа.
20. Протоколы аутентификации без разглашения.
21. Использование хэш-функций. Одноразовые подписи на цепочках Лампорта и на дереве Меркле.
22. Слепая подпись Чаума и ее использование в протоколах электронного голосования.
23. Стеганография. Основные свойства, подходы к реализации, использование алгоритмов LSB и психовизуальных/психоаккустических эффектов.
24. Атаки на стеганографические методы. Понятие цифрового водяного знака.
25. Потоковые шифры. Использование регистров сдвига с линейной обратной связью и их суперпозиций. Понятие линейной сложности и профиля линейной сложности. Расчет линейной сложности.
26. Стандарт шифрования в GSM A5. Принцип построеия основные свойства, известные атаки.
27. Методы и протоколы защиты информации от несанкционированного использования и копирования.
28. Классификация вредоносных программ. Классические определения четырех основных типов вредоносных программ. Методы борьбы с вредоносными программами.
29. Постквантовая криптография как отдельный раздел криптографии. Основные концепции и идеи.
30. Технология блокчейн. Принцип работы. Публичный и приватный блокчейн.
31. Проблемы безопасности сетевых технологий. Сетевая модель OSI/ISO. Уровни модели OSI.
32. Риск информационной безопасности: понятие; задача управления рисками; методологические основы и инструментальные средства оценки рисков информационной безопасности, остаточные риски.
33. Состязательное и вредоносное машинное обучение. Методы противодействия атакам на нейросети и машинное обучение.
34. Основные угрозы безопасности веб-ресурсов. OWASP Top 10: описание и механизмы защиты.
35. Методы и методики тестирования на проникновение; Основы деятельности SOC в организации. Понятия Red team, Blue team, Purple team; MITRE ATT&CK Framework.
36. Обзор информационных ресурсов в области информационной безопасности: авторы, фундаментальные монографии и статьи, нормативно-правовые документы, ресурсы научных школ, профессиональные сообщества.