Доклады семинара «Теория автоматов»

В первом полугодии 2026 года на научном семинаре «Теория автоматов» под руководством профессора Эльяра Эльдаровича Гасанова состоялось 18 докладов.

11 февраля 2026 года

О конфигурации паросочетаний, ее свойствах и приложении в криптографии

инж. 1 кат. А. И. Болотников

В рамках доклада автор представит новую конструкцию — конфигурацию паросочетаний, и проведет обзор свойств конфигурации паросочетаний и ее характеристического многочлена. Также будет сформулирована задача о неправильной функции весов, показана ее NP-полнота и построение на ее основе системы шифрования Болотникова-Ирматова (криптосистемы паросочетаний).

18 февраля 2026 года

Сложность проблемы сюръективного гомоморфизма для циклов

инж. 1 кат. Н. П. Корчагин

Для графа H в задаче Surj-Hom(H) по данному графу G требуется определить, существует ли сюръективный гомоморфизм из G на H. Доклад посвящен сложности задачи Surj-Hom для графов, которые получаются из неориентированных циклов добавлением ориентации некоторым ребрам и в которых каждая вершина содержит петлю. Будет представлен обзор задачи, включая современные достижения и результаты докладчика. Задача рассматривается как частный случай массовой задачи сюръективного удовлетворения ограничениям SCSP. Вводится ряд свойств, которые для множества отношений Γ позволяют определять сложность SCSP(Γ) с помощью сведения или путем анализа функций, сохраняющих эти отношения. Введенные свойства используются, чтобы определить сложность задачи для всех рассматриваемых графов, кроме шести циклов длины 4, 5 и 6.

25 февраля 2026 года

О трех начальных приближениях к формальному определению визуального образа в произвольной визуальной среде

проф. В. Н. Козлов

Распознавание визуальных образов — одна из центральных задач для интеллектуальных систем. Продвижению здесь математических, теоремных методов исследования в немалой степени мешает отсутствие полного и приемлемого формального определения понятия визуального образа в произвольной визуальной среде. На содержательном, интуитивном уровне ясно, что зрительный образ — понятие сложное, многоплановое и многоуровневое, и вряд ли определение образа может быть дано некоторым «единовременным» усилием. В докладе будет представлена идея подхода к определению образа последовательными приближениями, и описаны три начальных приближения.

4 марта 2026 года

Формальная верификация протоколов консенсуса с византийской отказоустойчивостью

асп. К. В. Зиборов

Протоколы консенсуса являются фундаментом блокчейн-технологий, обеспечивая согласованность данных в распределенных сетях. В условиях византийских отказов, когда часть узлов может вести себя злонамеренно, ошибки в дизайне таких протоколов приводят к нарушениям критических свойств согласованности и живучести. В рамках работы проработана методология формальной спецификации и верификации BFT-протоколов с использованием метода проверки модели, позволяющая получать более строгие гарантии корректности.

Помимо классических гарантий, вводится строгая формализация устойчивости к цензуре для BFT-протоколов с лидером как ограниченной гарантии качества цепочки; показано, что стандартная ротация лидера может приводить к нарушению этой гарантии. Предлагается и формально верифицируется правило выбора лидера, обеспечивающее устойчивость к цензуре без ослабления исходных гарантий безопасности и живучести. Предложенная методология проверена на примерах индустриальных протоколов IBFT и SmartBFT.

11 марта 2026 года

Преодоление ограничений обучения сиамских нейронных сетей в задаче оптического распознавания символов

асп. А. К. Мокин

Метрическое обучение находит широкое применение в современных задачах, таких как оптическое распознавание символов (OCR), идентификация лиц и рекомендательные системы. Доклад посвящен преодолению возникающих в ходе решения таких задач практических проблем, связанных с обучением сиамских нейронных сетей. В качестве примера будет рассмотрена задача OCR и ограничения существующих методов и подходов, из-за которых сиамские сети могут работать хуже и чаще ошибаться, например, при распознавании рукописного текста с большой вариативностью или визуально похожих классов. Будут представлены способы адаптации обучения для достижения высокой точности при небольших данных и преодоления ограничений известных методов и подходов.

18 марта 2026 года

Проблема полноты в классе линейных дефинитных автоматов

асп. И. В. Молдованов

Рассматриваемый в докладе класс линейных дефинитных автоматов возникает путем замыкания по операциям суперпозиции системы, состоящей из сумматора и задержек с заданным начальным состоянием. Этот класс представляет интерес тем, что, в отличие от класса линейных автоматов, содержит конечные полные системы относительно операций суперпозиции. Ранее для конечнопорожденных подмножеств этого класса, содержащих нулевую константу, был получен критерий полноты в терминах системы замкнутых классов, а также предложен алгоритм распознавания полноты. В докладе этот результат обобщается: путем расширения системы замкнутых классов получен критерий полноты для произвольных подмножеств класса линейных дефинитных автоматов. На его основе может быть построен алгоритм распознавания полноты произвольных конечных подмножеств данного класса.

25 марта 2026 года

Методы построения представлений объектов с использованием внешней информации о свойствах наборов объектов

м.н.с. А. М. Колосов

В докладе рассматриваются методы построения представлений объектов с использованием внешней информации о свойствах наборов объектов. Актуальность работы связана с тем, что задачи построения, снижения размерности, бинаризации и улучшения качества векторных представлений играют важную роль в машинном обучении и анализе данных. В центре внимания находится постановка задачи обобщенного неметрического многомерного шкалирования, в которой в качестве входных данных используются не сами близости между объектами, а сведения о порядке близостей в парах пар объектов. На этой основе предлагаются методы построения представлений, а также методы снижения размерности, бинаризации и улучшения качества уже имеющихся векторных представлений. Отдельное внимание уделяется использованию методов машинного обучения, позволяющих получить единый подход к решению этого круга задач. Представленные результаты показывают практическую значимость предложенных методов и их применимость к различным типам данных.

1 апреля 2026 года

Об одном необходимом условии устойчивости криптосистемы паросочетаний

доц. А. А. Ирматов, инж. 1 кат. А. И. Болотников

В докладе рассматривается составная часть секретного ключа криптосистемы паросочетаний — функция весов, для которой задача о чередующемся взвешенном пути решается за полиномиальное время. Значительная часть координат векторов весов данной функции используется в качестве «шума» для усложнения взлома всей системы шифрования. В докладе будет представлено условие на «шум», необходимое для устойчивости системы к атакам, опирающимся на размерность специальных подмножеств векторов весов.

Подбор оптимальной схемы квантизации нейронных сетей с помощью градиентных методов

с.н.с. В. С. Половников, асп. Д. Н. Давыдова

Квантизация является одной из основных техник оптимизации и ускорения больших языковых моделей, но подбор разрядности вручную или перебором для каждого слоя нейронной сети был бы слишком долгим и затрачивал бы слишком много вычислительных ресурсов. Доклад будет посвящен применению метода дифференцируемого поиска архитектуры нейронной сети (DARTS) для подбора оптимальной схемы квантизации генеративной языковой модели, будут приведены результаты экспериментов. В отличие от оригинального DARTS, вместо архитектурных параметров с помощью градиентного спуска подбираются оптимальный метод квантизации и разрядность для каждого линейного слоя модели.

Устойчивость нечеткой классификации пользователя для определения уровня физических нагрузок

проф. А. П. Рыжов, студ. А. С. Гусев

В работе исследуется устойчивость нечеткого вывода Мамдани относительно параметров функций принадлежности. Рассматривается ситуация, когда функции принадлежности заданы с некоторой возможной ошибкой, и оценивается влияние этой ошибки на результат вывода. Такая ситуация характерна для экспертного задания функций принадлежности и проблемы холодного старта. На примере классификации физического состояния пользователя по данным pose estimation показано, что нечеткий вывод позволяет корректно интерпретировать данные, полученные трекингом ключевых точек тела. Установлено, что малые ошибки в заданиях функций принадлежности не приводят к существенным ошибкам вывода, что гарантирует корректность работы систем нечеткого вывода в рассматриваемых условиях.

Нечеткая агрегация рисков на деревьях с использованием t-норм

проф. А. П. Рыжов, студ. Ф. А. Федотов

В работе рассматривается задача нечеткой агрегации рисков в иерархических структурах, моделируемых ориентированными деревьями, с использованием t-норм. Исследуются строгие архимедовы t-нормы и их представление через аддитивные генераторы, что позволяет получить аналитические формулы для итоговой агрегированной оценки и для

ее чувствительности к изменениям листовых значений. На этой основе вводятся и анализируются характеристики устойчивости к шуму, селективности инцидентов и уровневой детекции событий. Также обсуждаются общие подходы к выделению и конструированию классов операторов агрегации, согласованных с требованиями робастности и чувствительности.

8 апреля 2026 года

Аналог цифровой подписи для буквенных текстов на основе инвариантов аффинных преобразований для алфавитных изображений

проф. В. Н. Козлов

Как правило, сердцевиной цифровой подписи является функция, у которой ее значение при заданном значении аргумента вычисляется легко, а обратное, т.е. вычисление значения аргумента при известном значении функции, трудно. В докладе будет представлен аналог цифровой подписи для буквенных текстов на другой принципиальной основе, с использованием вводимого понятия алфавитного изображения и кодов изображений, определяющих их с точностью до аффинных преобразований.

15 апреля 2026 года

Предполные классы в классе полиномов четырехзначной логики, содержащие все полиномиальные функции одной переменной

студ. И. М. Янушкевич

В работе исследовались полиномы в четырехзначной логике. Было получено взаимно-однозначное соответствие между полиномами в четырехзначной логике и булевыми функциями той же арности. С помощью полученного соответствия были описаны два предполных класса, содержащие все полиномиальные функции одной переменной. Один из них можно считать аналогом класса Слупецкого.

Реализация булевых функций и операции сложения в клеточных автоматах с локаторами

студ. Ч. А. Надиров

Клеточный автомат с локаторами — это обобщение классического клеточного автомата, в котором ячейки могут обмениваться информацией не только с соседями, но и на расстоянии с помощью сигналов. В работе

разработан алгоритм сложения нескольких натуральных чисел в этой модели, работающий за время, пропорциональное логарифму от числа слагаемых. Также доказано, что почти все булевые функции можно реализовать клеточными автоматами с локаторами со сложностью 2^n, причем эта сложность неулучшаема по порядку, а время вычисления значения функции занимает всего 2 такта.

22 апреля 2026 года

Задача подсчета точек клеточными автоматами с локаторами

студ. А. Е. Бобров

В работе исследуются клеточные автоматы с локаторами. Предложены алгоритмы подсчета количества точек на плоскости и извлечения квадратного корня числа, время выполнения которых логарифмически зависит от величины обрабатываемого множества/входного значения.

О сложности булевых операторов в некоторых классах клеточных схем

студ. Д. Э. Каламбетов

Клеточные схемы — структуры, где элементы расположены по решетке и могут взаимодействовать только с соседними элементами. В работе рассматриваются клеточные схемы с бинарными значениями входов и выходов, но с элементами арифметического сложения и без ограничения на значность передаваемых через проводники сигналов. Найдены порядки роста сложности дешифратора в классе клеточных схем из линейных элементов, элемента Хэвисайда и элементов, вычисляющих определенные разряды целых неотрицательных чисел, а также двоичного умножителя в классе клеточных схем из кусочно-линейных элементов, в том числе в конечном базисе.

Об алгоритмах построения групп автоморфизмов нагруженных графов, мультиграфов и гиперграфов

студ. Е. И. Яковенко

В докладе будет рассмотрен алгоритм МакКея, используемый для построения систем образующих групп автоморфизмов графов. Алгоритм распространен на нагруженные графы, мультиграфы и гиперграфы, возникающие при анализе молекулярных структур в химии. Рассмотрены примеры применения разработанного алгоритма к молекулярным графам.

6 мая 2026 года

Минионы и алгоритмы для решения задачи удовлетворения ограничениям

с.н.с. Д. Н. Жук

Открытия 2025 года показали, что почти любой универсальный алгоритм для задачи удовлетворения ограничениям задается абстрактным минионом, а применимость алгоритма зависит от существования гомоморфизма минионов. В докладе мы покажем, как абстрактные минионы возникают из замкнутых классов функций k-значной логики, продемонстрируем на примерах, как минионы задают конкретные алгоритмы. На примере классификации Шефера мы покажем, как наличие гомоморфизма минионов связано с применимостью алгоритма. В конце мы сформулируем конкретные (почти комбинаторные) вопросы, решение которых станет прорывом в теории алгоритмов.