

Научно-исследовательский семинар «*Математические вопросы кибернетики*»

В пятницу, **14 марта 2025 г.**, состоится доклад:

Галатенко Алексей Владимирович (Москва, МГУ имени М.В. Ломоносова)

«О некоторых свойствах конечных квазигрупп».

Аннотация доклада. Конечные квазигруппы являются перспективной платформой для реализации различных криптоалгоритмов. Для обеспечения стойкости на квазигруппы накладывается ряд требований. В.А. Артамонов предложил использовать полиномиально полные квазигруппы (то есть такие, что квазигрупповая операция и множество всех констант порождают с помощью суперпозиции все функции) без собственных подквазигрупп. В докладе приводится критерий полиномиальной полноты, анализируется типичность свойств полиномиальной полноты и отсутствия собственных подквазигрупп, рассматриваются методы построения полиномиально полных квазигрупп без подквазигрупп, оценивается сложность распознавания соответствующих свойств; в заключение обсуждается перенос результатов на случай n -арных обобщений квазигрупп — конечных n -квазигрупп.