Научно-исследовательский семинар ***«Математические вопросы кибернетики»***

В пятницу, **17 ноября 2023 г.**, состоится доклад:

Царегородцев Кирилл Денисович (Москва, МГУ имени М. В. Ломоносова)

«Правильные семейства дискретных функций: эквивалентные определения и свойства».

Аннотация доклада. В последнее время растет интерес к использованию в криптографических (и теоретико-кодовых) приложениях некоммутативных и неассоциативных алгебраических структур (в частности, квазигрупп). Задание квазигруппы в виде «таблицы умножения» непрактично, поскольку размер требуемой для ее хранения памяти растет крайне быстро при росте «длины» перемножаемых элементов. Одним из возможных вариантов обойти это ограничение является функциональное задание квазигрупповой операции, при котором координаты произведения $(z_1, \dots, z_n)$ задаются функциями от координат сомножителей: $z_i = f_i(x_1, \dots, x_n, y_1, \dots, y_n)$.

Для функционального задания квазигрупповых операций В.А. Носовым в 1999 году было введено понятие правильного семейства (булевых) функций. Исходное определение было расширено сначала на случай абелевых групп, а затем и на более общие алгебраические структуры. В докладе мы рассмотрим исходное определение понятия правильного семейства, некоторые примеры таких семейств, а также результаты, полученные в последние годы: альтернативные характеризации правильных семейств (с более «геометрических» точек зрения), некоторые их свойства (оценки количества правильных семейств, результаты о конкретных классах правильных семейств).