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

В пятницу, **19 мая 2023 г.**, состоится доклад:

Таранников Юрий Валерьевич (Москва, МГУ имени М. В. Ломоносова)

«Конструкции и свойства корреляционно-иммунных и платовидных булевых функций».

Аннотация доклада. Доклад представляет собой обзор результатов автора. С помощью математических подходов изучены параметры криптографически важных функций, в первую очередь корреляционно-иммунных и платовидных, установлены оценки на эти параметры и на их взаимосвязь между собой. Построены функции, обладающие криптографически хорошими параметрами, в том числе экстремальными, в широких диапазонах значений. Предложены эффективные схемные и программные реализации таких конструкций. Получены эффективные оценки, асимптотические и точные формулы для числа функций из криптографически важных классов и вспомогательных комбинаторных объектов, включая разбиения пространства на аффинные подпространства.