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

В пятницу, **11 ноября 2022 г.**, состоится доклад:

Козлов Вадим Никитович (Москва, МГУ имени М.В. Ломоносова)

«Цифровая подпись на основе кодов, определяющих изображения с точностью до аффинных преобразований».

Аннотация доклада. Первый «допотопный» вариант защиты документа от подделки (используется, однако, и поныне) — это так называемая «живая» подпись (или факсимиле) и канцелярская печать. Но в наши дни документооборот большей частью электронный и, зачастую, с очень большим числом документов (электронные торги, банковские платежные системы, сделки в криптовалютах и пр.). Факсимиле в этом случае неудобно, а главное — крайне ненадежно. Здесь работает возникшая около тридцати лет назад цифровая подпись (или электронная цифровая подпись — ЭЦП). Как правило, сердцевиной этой конструкции, т. е. ЭЦП, является функция, у которой ее значение при заданном значении аргумента вычисляется легко, а обратное, т. е. вычисление значения аргумента при известном значении функции, очень трудно.

В докладе описывается аналог цифровой подписи на другой принципиальной основе — на использовании кодов, определяющих изображения с точностью до аффинных преобразований.