Семинар “Криптография и теория чисел”

Лаборатория “Математические методы защиты и обработки информации”

Известно, что многие современные криптосистемы, в т.ч. и стандартизированные в РФ, могут быть взломаны при помощи квантовых вычислений. Этим обусловлена современная мировая тенденция поиска и стандартизации новых алгоритмов, устойчивых к квантовым атакам. Цель семинара – изучить эти новые (“постквантовые”) криптографические примитивы, понять их сильные и слабые стороны. Вместе мы узнаем, как выполняется криптоанализ и доказательство безопасности криптографических протоколов. В рамках семинара вы сможете провести собственное исследование и опубликовать его результаты в научном журнале.

Приглашаем всех заинтересованных студентов, аспирантов и преподавателей. Входной порог – алгебра (группы, кольца, конечные поля). Основные предварительные сведения расскажем.

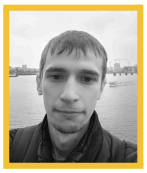
В программе семинара:

- Обзор постквантовых криптосистем-кандидатов на стандартизацию института NIST;
- Криптоанализ схем на алгеброгеометрических кодах, Classic McEliece;
- Атаки на криптосистему McEliece, предлагаем свои модификации атак!

Орг. собрание: Среда 22.01.2025 в 17:00 ауд. 210 (время скорректируем).

- Запись не нужна, просто приходите, следите за новостями в Telegram-канале.

Руководители семинара:

к.ф.-м.н., доцент **Новоселов Семен** **Александрович**	
мл. науч. сотрудник **Колесников Никита** **Сергеевич**	

Подробнее на странице семинара:
crypto-kantiana.com/events/seminar

Telegram-канал:
t.me/crypto_seminar