Алгебраично-вероятностные методы исследования стойкости и эффективности криптографических алгоритмов и протоколов.

1. **Номер государственной регистрации – 0108U001549.**

2. **Научный руководитель -** д.ф-м.н. Савчук М.М

3. **Результаты**

Цель работы заключается в разработке и усовершенствование алгебраично-вероятностных методов исследования криптографических преобразований, анализа симметричных и асимметричных алгоритмов шифрования, способов автентификации, криптографических протоколов, с учетом последних достижений криптологии и применения результатов для оценки стойкости и эффективности современных криптосистем и криптографических протоколов, усовершенствования методов криптографической защиты информации. Разработаны эффективные алгоритмы решения линейных систем уравнений над конечными полями с искажениями; алгоритмы решения целочисленных уравнений специального вида. Усовершенствованы и разработаны инновационные методы и программы алгебраических атак на поточные шифры. Получены оценки характеристик булевых функций, односторонних функций. Разработаны методы криптоанализа, которые оптимально используют корреляционные зависимости, алгебраические методы и средства перебора. Созданы новые критерии для проверки криптографического качества последовательности