ДСТУ 7564:2014 – новітній алгоритм криптографічного гешування і потребує детального дослідження.

Мета роботи: розробка та впровадження нових моделей та методів оцінювання стійкості геш-функції ДСТУ 7564:2014 до сучасних криптоаналітичних атак.

Завдання дослідження: побудова rebound-атаки на алгоритм ДСТУ 7564:2014 та оцінювання стійкості до побудованої атаки.

Rebound-атака – це метод диференціального криптоаналізу геш-функцій, що полягає у побудові диференціальних шляхів у стискаючих відображеннях та їх використанні для пошуку колізії геш-функції. (застосовано для Грьостл)

Для вирішення поставленої задачі необхідно побудувати диференціальні шляхи для 5 і 6 раундів функції стискання ДСТУ 7564:2014. Засновуючись на них побудувати rebound-атаку на геш-функцію ДСТУ 7564:2014 і отримано оцінки стійкості до rebound-атаки на 5 і 6 раундів функції стискання алгоритму гешування.