

**РЕЦЕНЗІЯ**  
**на магістерську атестаційну роботу студента гр. БІКСм-12-1**  
**Фролова Владислава Володимировича**  
**на тему:**  
**“Дослідження методів формування нелінійних вузлів заміन блочних симетричних шифрів”**

Магістерська атестаційна робота виконана згідно завдання у повному об’ємі та з відмінною якістю. Робота відповідає стандартам та вимогам, які ставляться до магістерських атестаційних робіт, містить посилання на актуальні публікації та статті з даної тематики, в тому числі іншомовні. Огляд доступних науково-технічних джерел інформацій та їх цитування зроблене на необхідному рівні.

Основні результати роботи опубліковані в статтях в збірниках наукових праць, одержали схвалення фахівців. Рішення поставлених у роботі задач обґрунтовані і відрізняються повнотою та доступністю для сприйняття.

Необхідно зазначити, що робота має практичну спрямованість отриманих результатів з оцінки ефективності методів формування нелінійних вузлів заміन блочних симетричних шифрів, а саме методу імітації відпалу. В роботі були розглянуті сучасні алгоритми шифрування з метою оцінки ефективності формованих вузлів замін та наочно відображені порівняльні криптографічні та швидкісні характеристики методу імітації відпалу.

При дослідженнях продемонстровано високий рівень програмного моделювання, що дозволило отримати важливі статистичні та практичні результати. В роботі є подальші напрямки розвитку та вона може бути доповнена і розвинута.

Недоліком роботи є недостатнє висвітлення порівняльного аналізу методу імітації відпалу з іншими методами формування нелінійних вузлів змін.

Вважаю, що магістерська атестаційна робота заслуговує оцінки «відмінно», а студент Фролов Владислав Володимирович присвоєння звання магістра, кваліфікації інженера з безпеки інформаційних та комунікаційних систем з дослідницьким рівнем діяльності, викладача ВНЗ.

**Рецензент:** доцент ХНТУСГ, кандидат технічних наук, доцент Кошман С.О.

“        ”        2013р.

\_\_\_\_\_

(підпис)