

РЕЦЕНЗІЯ

на бакалаврську атестаційну роботу студента гр. БІКС-08-1

Кіянчука Р. І.

на тему:

“Аналіз криптографічних властивостей симетричних шифрів”

У роботі проведено аналіз симетричних шифрів, що проходять міжнародну стандартизацію та є перспективними для використання в сучасних системах захисту. Розглянуто можливість використання шифрів ГОСТ 28147 та PRESENT у сфері мало-ресурсної (lightweight) криптографії. Досліджено стійкість шифра ГОСТ проти алгебраїчного криптоаналізу та розроблено програмний комплекс з побудови та вирішення нелінійної системи рівнянь криптоалгоритму.

Робота виконана згідно завдання у повному об'ємі, з відмінною якістю та відповідає стандартам і вимогам, що ставляться до бакалаврських атестаційних робіт. Основні результати роботи є новими та актуальними в сучасній криптографії, доповідались на міжнародних науково-практичних конференціях.

Достовірність результатів підтверджується експериментальними дослідженнями та доступним програмним кодом реалізації розроблених методів.

Вважаю, що робота заслуговує оцінки «відмінно», а її автор, Кіянчук Руслан Ігорович, присвоєння звання бакалавра з захисту інформації в інформаційних та комунікаційних системах.

Рецензент :

“ _____ ” 2010р.

(підпис)