ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

ВІДГУК

на магістерську атестаційну роботу студента

Фролова Владислава Володимировича

Спеціальність 8.17010101
“Безпека інформаційних та комунікаційних систем”

Тема магістерської атестаційної роботи
“Дослідження методів формування нелінійних вузлів замін
блочних симетричних шифрів“

Магістерська атестаційна робота Фролова В.В. присвячена вирішенню актуального практичного завдання – дослідження методів формування нелінійних вузлів замін, оцінка оптимальних криптографічних показників сформованих вузів замін та оцінка ефективності швидкодії методу імітації відпалу. Вирішення проблем криптографічної стійкості шифрів – це основне завдання сучасної криптографії, тому тема магістерської роботи є актуальною.

При роботі над магістерською роботою студент розробив програмну реалізацію оцінки криптографічних показників нелінійних блоків замін, метод імітації відпалу та метод випадкової генерації з фільтруванням.

До основних результатів роботи слід віднести дослідження та класифікація методів формування нелінійних вузлів замін, вдосконалення цінової функції, реалізація методу імітації відпалу та проведені порівняльні аналізи з оцінки підвищення стійкості шифрів MacGuffin, ГОСТ 28147-89 та продуктивності формування оптимальних вузлів замін відносно методу випадкової генерації.

Отримані результати викладені послідовно і систематично, стиль викладення ясний. Пояснювальна записка оформлена у відповідності з методичними вказівками до магістерської атестаційної роботи, термінологія та спеціальні позначення використані вірно, зміст відповідає завданню на магістерську атестаційну роботу.

При виконанні магістерської атестаційної роботи Фролов В.В. показав вміння самостійно освоювати новий матеріал, аналізувати та систематизувати отримані результати, робити за ними обґрунтовані висновки, продемонстрував вміння працювати з сучасною науково-технічною літературою і інформацією, яка доступна у мережі Інтернет. Студент вільно володіє сучасними комп’ютерними та телекомунікаційними системами, працював наполегливо і самостійно, виявляв ініціативу.

Фролов В.В. проявив себе як сформований спеціаліст і здатний до самостійної роботи у галузі інформаційної безпеки. Магістерська атестаційна робота виконана на високому рівні, відповідає вимогам до магістерських атестаційних робіт і може бути подана у Державну екзаменаційну комісію до захисту.

Керівник магістерської атестаційної роботи _____ д.т.н., проф. Кузнецов О.О.

“___” _____ 2012 р.