

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

ВІДГУК

на бакалаврську роботу студента

Кіянчука Руслана Ігоровича

Спеціальність 6.1701

«Безпека інформаційних та комунікаційних систем»

Тема бакалаврської роботи

«Аналіз криптографічних властивостей симетричних шифрів»

Бакалаврська робота Кіянчука Р. І. присвячена аналізу сучасного стану симетричних шифрів, дослідженню їх криптографічних властивостей та вирішенню практичного завдання – розробки програмного комплексу для алгебраїчного криптоаналізу шифра ГОСТ 28147-89. Незважаючи на розвинутість теоретичних знань у сфері криптографії, сучасні системи захисту часто використовують ненадійні шифри та протоколи для забезпечення захисту інформації. Отже перед впровадженням у якості стандарту криптографічні примітиви мусять підлягати аналізу стійкості, тому тема бакалаврської роботи є актуальною. Існуючі програмні рішення дозволяють виконувати алгебраїчний аналіз шифрів, що є міжнародними стандартами (AES, PRESENT) та не придатні для роботи з криптоалгоритмом ГОСТ, стандартом шифрування країн СНД. Програмна реалізація побудови алгебраїчної системи шифру ГОСТ є необхідною для застосування сучасних методів криптоаналізу з метою подальшого дослідження криптоалгоритму.

При роботі над бакалаврською роботою студент розробив модель загроз і модель порушника, виконав огляд сучасних технологій для побудови систем виявлення вторгень, комерційних і вільних засобів, розробив і протестував рішення для захисту мереж малого та середнього бізнесу.

До основних результатів роботи слід віднести систематизований огляд сучасних технологій і засобів побудови систем виявлення вторгень, розроблену систему виявлення вторгень. Отримані результати викладені послідовно і систематично, стиль викладення ясний. Пояснювальна записка оформлена у відповідності з методичними вказівками до дипломної роботи, термінологія та спеціальні позначення використані вірно, зміст відповідає завданню на дипломну роботу.

При виконанні дипломної роботи Кіянчук Р. І. 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.

Кіянчук Р. І. проявив себе як сформований спеціаліст, здатний до самостійної роботи у галузі інформаційної безпеки. Дипломна робота виконана на високому рівні, відповідає вимогам до дипломних робіт і може бути подана до Державної екзаменаційної комісії для захисту.

Керівник дипломної роботи

доц. Халімов Г. З.

“ 14 ” травня 2012 р.