РЕЦЕНЗІЯ

на наукову роботу шифр «Потоковий шифр», представлену на Конкурс зі спеціальності 125 Кібербезпека

№ з/п	Характеристики та критерії оцінки рукопису наукової роботи	Максимальна кількість балів (за 100-бальною шкалою)	Бали
1	Актуальність проблеми	10	5
2	Новизна та оригінальність ідей	15	5
3	Використані методи дослідження	15	5
4	Теоретичні наукові результати	10	2
5	Практична направленість результатів (документальне підтвердження впровадження результатів роботи)	20	5
6	Рівень використання наукової літератури та інших джерел інформації	5	2
7	Ступінь самостійності роботи	10	5
8	Якість оформлення	5	1
9	Наукові публікації	10	0
10	Недоліки роботи (пояснення зниження максимальних балів у пунктах 1-9):		
10.1	Наведені у вступі до роботи відомості не стосуються розв'язаних у роботі задач. У роботі взагалі не розглядається проблематика, пов’язана із закладками (бекдорами) та клептографічними механізмами, про які розлого розповідається у вступі.		
10.2	Використання динамічно змінюваних S-блоків – відома ідея; авторський підхід претендує на певну оригінальність		
10.3	Основну частину результатів, одержаних у роботі, складають результати експериментальних досліджень. Однак у роботі відсутні будь-які відомості про сам статистичний експеримент: об’єм вибірки, джерело даних, кількість використаних ключів для шифрів, джерело ключів, безпосередньо дані обчислень тощо. Наведені статистичні профілі неможливо порівнювати між собою, оскільки для деяких графіків крок відображення складає 0,005, а для інших – 0,2 (хоча значення, які наводяться на графіках, з однакового діапазону).		
10.4	Основним теоретичним результатом роботи є деяке вдосконалення режиму гамування шифру ГОСТ, яке насправді модифікує сам алгоритм шифрування та ставить його в залежність від вхідних даних (що вважається дуже поганою практикою). У роботі відсутнє обґрунтування обраному вдосконаленню та бодай якийсь теоретичний аналіз властивостей модифікованого шифру. Більш того, модифікація викладена із використанням термінів та позначень, які не були введені перед цим (стор. 14): код Sm, таблиці $H_0..H_3$, значення S_{255} тощо. Це не просто ускладнює розуміння запропонованої модифікації, а робить прямо неможливим її аналіз. У експериментальній частині (розділ 3, стор. 15) зазначається: «В роботі було запропоновано три режими формування псевдовипадкової послідовності в удосконаленному алгоритмі при К=1, К=2, К=3». При цьому єдине місце, де фігурував параметр К – це стор. 12: «В даній схемі використовується блок підстановки К, який складається з 8 статичних блоків заміни»; відповідно, масив з 8 блоків заміни не може дорівнювати 1, 2 чи 3.		
10.5	Запропонований модифікований шифр ГОСТ потенційно може бути використаний на практиці після суттєво більш ретельного аналізу		
10.6	У переліку використаних джерел присутні ненаукові джерела ([1-4]).		
10.7	Вступ та перший розділ роботи не стосуються викладених в подальшому результатів. Вступ містить прямі текстові запозичення з джерела [3], перекладені з російської, без належного посилання, що є ознакою порушення академічної доброчесності. Також		

	робота містить текстові запозичення з інших джерел, не вказаних у переліку, наприклад, https://ko.com.ua/o_novom_ukrainskom_standarte_shifrovaniya_110863 Наведений на стор. 11-12 опис режиму гамування ГОСТ дослівно перекладений з тексту стандарту та не є необхідним для викладення результатів.
10.8	Оформлення роботи місцями порушує стандарти оформлення наукових робіт. У роботі не сформульовані мета та завдання дослідження, об'єкт, предмет та методи дослідження. Робота містить численні неточності як граматичного характеру (зокрема, багато недоперекладених з російської слів), так і змістовного, наприклад, твердження, що ДСТУ ГОСТ 28147:2009 втратив статус стандарту у 2014 році, твердження, що режим гамування відповідає режиму OFB (насправді він відповідає режиму лічильника) тощо.
10.9	Не наведено наукових публікацій автора за темою роботи
Сума балів	30

Загальний висновок: не рекомендується до захисту на науково-практичній конференції.

Рецензент

_____ _____ 20____ року