РЕЦЕНЗІЯ

на наукову роботу шифр «AES», 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	8
2	Новизна та оригінальність ідей	15	12
3	Використані методи дослідження	15	12
4	Теоретичні наукові результати	10	5
5	Практична направленість результатів (документальне підтвердження впровадження результатів роботи)	20	10
6	Рівень використання наукової літератури та інших джерел інформації	5	4
7	Ступінь самостійності роботи	10	10
8	Якість оформлення	5	4
9	Наукові публікації	10	10
10	Недоліки роботи (пояснення зниження максимальних балів у пунктах 1-9):		
10.1	Необхідність розглядати лавинні критерії для функцій q-значної логіки саме у криптоаналізі шифру AES не обґрунтована належним чином. Уся архітектура шифру AES побудована на булевих функціях та перетвореннях у байтових скінченних полях; застосування функцій q-значної логіки при аналізі такої конструкції є зовсім неочевидним.		
10.2	Проблема аналізу криптографічних властивостей S-блоків є відомою; у роботі пропонуються ідеї творчого характеру для їх розв’язання		
10.3	Методи дослідження використано коректно, але не в повній мірі; зокрема, було зосереджено увагу лише на одному сімействі криптографічних параметрів, хоча криптографічно якісні S-блоки повинні задовольняти багатьом вимогам, які, на жаль, часто конфліктують. (Також див. зауваження п. 10.4)		
10.4	Теоретичним науковим результатом роботи є метод побудови S-блоків, які мають гарні лавинні властивості. Однак запропонована процедура побудови наведена без жодного обґрунтування та/або доведення (окрім репліки «Неважко переконатися», стор. 20), що у результаті її роботи дійсно генерується S-блок із заданими властивостями. З тексту роботи випливає, що усі перевірки виконувались експериментально; відповідно, не зовсім зрозуміло, чим керувались автори при формулюванні процедури побудови S-блоків.		
10.5	Робота носить теоретично-експериментальний характер, однак запропонований метод генерування S-блоків та результати експериментальних досліджень можуть знайти своє місце у практичних задачах криптоаналізу		
10.6	Перелік джерел містить лише деякі загальновідомі джерела з булевих функцій та роботи одного автора (можливо, наукового керівника роботи)		
10.8	Текст роботи містить русизми, які дуже ріжуть око: «уявлення S-блоків» замість «представлення», «суворий лавинний критерій» замість «строгий» тощо.		
10.9	Представлено дві публікації іноземною мовою		
Сума балів			75

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

Рецензент

_____ _____ 20____ року