До спеціалізованої вченої ради
ДФ 64.051.020 Харківського національного
університету імені В. Н. Каразіна

ВІДГУК

опонента доктора технічних наук, професора

КОВАЛЬЧУК ЛЮДМИЛИ ВАСИЛІВНИ

на дисертацію Лисицького Костянтина Євгенійовича

«МЕТОДИ ТА ЗАСОБИ ПОБУДОВИ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ З ПІДВИЩЕНОЮ СТІЙКІСТЮ ТА ШВИДКОДІЄЮ»,

представлену на здобуття ступеня доктора філософії за спеціальністю

122 – комп'ютерні науки

Актуальність теми. Блокові симетричні шифри можна вважати одним із основних інструментів, що забезпечує криптографічний захист інформації як у приватному, так і державному секторі, насамперед в таких критично важливих сферах, як транспорт, фінанси, армія тощо. Вони є невід'ємним компонентом сучасних систем криптографічного захисту інформації. Основна область їх використання - обробка великих обсягів конфіденційної інформації. А це серйозні вимоги до продуктивності систем захисту. Однією з основних вимог, які висуваються до сучасних і перспективних БСШ, є висока стійкість до відомих методів криптоаналізу, насамперед диференційного і лінійного. Конкурси з відбору перспективних блокових шифрів, що відбулися впродовж останнього десятиліття в Україні і в світі, наочно продемонстрували високу складність виконання такої експертизи і необхідність використання значних часових та інтелектуальних ресурсів. Крім того, задача створення стійких криптоалгоритмів набуває особливої актуальності з появою квантової криптографії.

Зазначені вище обставини обумовлюють актуальність дисертаційного дослідження Лисицького Костянтина Євгенійовича, яке сконцентровано на

питаннях удосконалення методів проєктування блокових симетричних шифрів з підвищеною стійкістю та швидкодією, у тому числі і у постквантовій криптографії.

Ступінь обґрунтованості наукових положень, висновків та рекомендацій, сформульованих у дисертації Лисицького К. Є., забезпечується використанням низки різноманітних методів пізнання, продуманою логікою викладення матеріалу, яка дозволила автору виконати поставлені перед собою завдання. Усі структурні елементи дисертації є взаємоузгодженими, об'єднані теоретично виваженою концепцією. Основні наукові положення дисертації відзначаються належною аргументованістю та достовірністю.

Здобувач, з точки зору окресленої теми, правильно визначив та сформулював об'єкт та предмет дослідження, продемонстрував знання методів наукового пізнання, що позитивно відбилося на повноті та всебічності дослідження, достовірності здобутих наукових результатів, їх науковій обґрунтованості, новизні розроблених теоретичних висновків і науково-практичних рекомендацій, винесених на захист. Так, об'єктом дослідження є процеси проєктування і створення блокових симетричних шифрів з підвищеною криптостійкістю і швидкодією для застосування в постквантовому періоді, а предметом дослідження — методи й засоби побудови блокових симетричних шифрів з підвищеною криптостійкістю і швидкодією для застосування в постквантовому періоді.

Використання різноманітних наукових методів на різних етапах дослідження дало змогу автору в повній мірі розкрити поставлені у роботі завдання та визначило цінність дослідження як в теоретичному, так і у практичному значенні. Обґрунтованість висновків та пропозицій здобувача забезпечена використанням широкого спектру загальнонаукових, міждисциплінарних та спеціальних методів наукового пізнання, а також широкою бібліографічною базою. Опрацювання суттєвої кількості наукових джерел (130 найменувань на 14 сторінках) дозволило дисертантові краще обґрунтувати наведені у роботі наукові результати і

пропозиції, що виносяться на захист. Позитивним аспектом роботи є використання англомовних джерел.

Обґрунтованість та достовірність сформульованих у дисертації висновків та пропозицій обумовлена також вдало продуманим планом роботи, який дає можливість розкрити проблематику. Зокрема, у першому розділі, присвяченому загальній характеристиці сучасного етапу розвитку технологій захисту інформації в Україні дисертант спочатку надає відомості та аналізує кращі проєктні рішення, потім зупиняється на особливостях сучасного етапу розвитку криптографії, зокрема постквантової, що дає можливість наприкінці розділу чітко та прозоро сформулювати задачі досліджень роботи.

Кожен наступний розділ містить стислий огляд попередніх результатів, що дозволяє сконцентрувати увагу на головному та полегшує сприйняття матеріалу.

Згідно з встановленими вимогами, кожний підрозділ завершується висновками, а загальні висновки сформульовані в кінці дисертаційного дослідження (стор. 181–187). Робота включає змістовні додатки.

Мета і завдання дослідження сформульовані у відповідності з темою дисертації. Загальний аналіз наукових праць, висновків за підрозділами та загальних висновків, основних наукових результатів дозволяє стверджувати, що заявлені завдання дисертантом було виконано, а поставлену мету — досягнуто.

Зв'язок роботи із науковими програмами, планами, темами. Як зазначається у вступі дисертаційної роботи Лисицького К. Є. результати роботи використані при виконанні ряду НДР. Відповідні акти реалізації зазначені у додатку.

Результати роботи втілені також в навчальний процес кафедри БІСТ національного університету імені В. Н. Каразіна при читанні дисципліни «Криптологічні методи в кібербезпеці» для магістрів спеціальності «Кібербезпека», а також для магістрів спеціальності «Безпека інформаційних і

комунікаційних систем», при курсовому проєктуванні з дисципліни «Прикладна криптологія», а також при виконанні магістерських дипломних робіт.

Наукова новизна положень дисертації насамперед зумовлена самим її характером. Цілком логічно та відповідно до встановлених вимог автор розпочинає дисертаційну роботу з огляду наукової літератури за темою дослідження. Заслуговує на підтримку комплексний підхід автора до аналізу стану наукових досліджень за обраною тематикою. Варто погодитись з висновками щодо особливостей побудування сучасних конструкцій БСШ та характеристикою стану сучасних технологій проєктування (**підрозділи 1.1–1.4**).

У **підрозділі 1.5**. дисертант звертається до аналізу можливостей застосування симетричної криптографії саме в постквантовому світі і приходить до необхідності вирішення протиріччя між вимогами підвищення стійкості і підвищення швидкодії сучасних БСШ.

Логічними є сформульовані в **підрозділі 1.6** задачі досліджень роботи.

У другому розділі дисертаційного дослідження «Обґрунтування нової методології оцінки стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу» Лисицький К. Є. розкриває сутність нової методології через обговорення специфічних умов приходу ітеративних шифрів до стаціонарного стану по комбінаторним показникам та диференціальним і лінійним властивостям. Такий підхід дозволив здобувачу визначити показники стійкості шифрів до атак диференціального та лінійного криптоаналізу, які будуть потрібні далі.

У третьому розділі «Розробка удосконаленої математичної моделі випадкової підстановки» даний підхід розвинено та удосконалено, що дозволило зробити висновки щодо можливості як S-блоки шифрів використовувати випадкові підстановки з виходу генератора випадкових підстановок, що проходять перевірку на відповідність додатним критеріям відбору. Ці нові

критерії запропоновані автором роботи. Тобто доведена можливість побудування шифрів, в яких без зниження стійкості можуть бути використані випадкові S-блоки.

Четвертий розділ роботи «Результати дослідження динамічних показників приходу блокових симетричних шифрів до стану випадкової підстановки» носить більш практичний характер. Автору належить сама методика виконання досліджень. Результати численних експериментів надані у вигляді таблиць. У розділі розв'язана задача уточнення і підтвердження за допомогою обчислювальних експериментів ефективності нової методики оцінки динамічних показників приходу блокових симетричних шифрів до стану випадкової підстановки, вперше отримані обґрунтовані об'єктивні дані для значень кількості циклів приходу до стану випадкової підстановки ряду сучасних шифрів.

У п'ятому розділі «Удосконалення методів проєктування блокових симетричних шифрів з підвищеною стійкістю і швидкодією» запропоновано ряд нових блокових симетричних шифрів (розробки запатентовано), в яких реалізовано всі попередні ідеї дисертаційної роботи. Це авторські розробки ШУП-1 та ШУП-2. Крім того, запропоновані шляхи удосконалення вже відомих алгоритмів.

В результаті виконаних досліджень розв'язана важлива науково-технічна задача, яка має практичне значення для вдосконалення технологій блокового симетричного шифрування.

На захист винесено 8 наукових результатів, серед яких 6 – запропоновано вперше.

Дисертаційна робота має практичне значення.

Розвинуті підходи та методи були використані для порівняльного аналізу шифрів, представлених у свій час на український конкурс з вибору національного

стандарту блокового симетричного шифрування, а також при дослідженні шифру Калина-2, що став національним стандартом України.

Результати роботи використані при виконанні науково-дослідних робіт Приватного акціонерного товариства «Інститут інформаційних технологій» (ЗАТ «ІІТ») Харківського національного університету радіоелектроніки та в наукових дослідженнях і навчальному процесі Харківського національного університету імені В. Н. Каразіна. Відповідні акти впровадження результатів досліджень надані в додатках.

Позитивно оцінюючи дисертацію Лисицького К. Є. «Методи та засоби побудови блокових симетричних шифрів з підвищеною стійкістю та швидкодією», водночас необхідно звернути увагу на деякі **дискусійні положення, висновки, пропозиції або такі, які вимагають додаткової аргументації автора**, а саме:

1. У роботі є ряд тверджень, що потребують уточнення, в частині умов та можливостей застосування невироджених підстановок при проєктуванні перспективних блокових симетричних шифрів. В основному твердження здобувача стосуються того, що невироджені s-блоки не впливають на стійкість блокового шифру. Можна навести приклади, які стосуються вироджених конструкцій. Наприклад, побудувати s-блоки таким чином, що ймовірність диференціалу для шифру з довільною кількістю раундів буде дорівнювати 1, або буде близькою до 1, що призведе до його швидкого зламу.

2. У роботі зустрічається термін «вироджені s-блоки», проте чіткого означення до цього терміну немає. У той же час, цей термін є важливим, оскільки, за твердженням автора, якщо s-блоки не є виродженими, то шифр буде стійким. Можна припустити, що до вироджених належать лінійні s-блоки. Але це буде лише припущенням, яке не дає відповіді на питання, які ще s-блоки автор називає виродженими.

3. Протягом роботи зустрічаються на наш погляд некоректні вислови та вирази. Особливо це стосується заголовків параграфів та таблиць. Наприклад, назва Таблиці 2.1 «…середні значення максимумів повних диференціалів».

4. При наведенні таблиць не завжди пояснюється, що саме є заповненням цих таблиць, або як отримані результати, що внесені у ці таблиці.

5. Певні питання викликає так званий інтегральний розподіл, яким користується здобувач. З тексту не зрозуміло, що він характеризує, чому і яка користь у використанні цього показника.

6. Незрозумілим є текст, що охоплює два останні абзаци сторінки 61 та три перші абзаци сторінки 62. Там говориться про некоректність визначення матриці перехідних імовірностей для марківського шифру за кілька раундів як добутку відповідних раундових матриць, і аргументом є те, що раунди містять нелінійні перетворення. Проте в даному випадку немає значення, які саме перетворення є в раунді, оскільки для марківських шифрів зазначена рівність є частковим випадком рівняння Колмогорова-Чепмена.

7. У роботі є певні граматичні та стилістичні помилки, наприклад, «атакуючі методи» замість «методи атак» (стор. 40), «мова йде не про вироджених їх конструкціях» (стор. 55), і т. ін.

Разом з тим, зазначені вище зауваження стосуються лише окремих положень дослідження, носять дискусійний, уточнюючий та рекомендаційний характер і не зменшують наукового та практичного значення дисертації.

Дисертація Лисицького К. Є. є самостійним, творчим, науковим дослідженням, в якому на основі аналізу теоретичних джерел та матеріалів практики отримані нові науково обґрунтовані результати, що в сукупності розв'язують задачу розробки удосконалених методів проєктування блокових симетричних шифрів з підвищеною стійкістю та швидкодією для умов постквантової криптографії.

Проведений аналіз змісту дисертації показує, що мета і завдання цього дослідження в цілому досягнуті та виконані, висновки і пропозиції в переважній більшості є обґрунтованими та доведеними. Структура роботи і її зміст є узгодженими. Зміст дисертації відображає основні положення, висновки та пропозиції, що винесені на захист.

Оформлення дисертації відповідає вимогам «Тимчасового порядку присудження ступеня доктора філософії», затвердженого постановою Кабінету міністрів України від 06.03.2019 р. № 167 (зі змінами), наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження вимог до оформлення дисертацій».

Ступінь апробації та впровадження результатів дисертаційної роботи. Основні теоретичні положення, висновки та пропозиції, що містяться в дисертації, доповідалися й обговорювались більш ніж на 6 міжнародних науково-практичних конференціях. Результати дисертаційного дослідження відображені у 11 статтях: 2 з них – в наукових фахових виданнях України; 2 – у закордонних виданнях, з яких одне входить до наукометричної бази SCOPUS; 2 – в науковому виданні України, що входить до наукометричної бази Web of Science.

В результаті аналізу дисертаційної роботи порушення академічної доброчесності не виявлено.

Висновок.

В цілому дисертаційна робота відповідає вимогам до робіт на здобуття ступеня доктора філософії. Взагалі, робота викладена технічно та математично грамотно. Основні результати дисертаційної роботи опубліковані у фахових виданнях. Відзначене дозволяє зробити висновок, що дисертаційна робота Лисицького Костянтина Євгенійовича є завершеною науковою працею, в якій отримані теоретичні та практичні результати, що по суті розв'язують наукову задачу розробки методів для удосконалення існуючих та побудови перспективних

блокових симетричних шифрів з підвищеною стійкістю та швидкодією для умов постквантової криптографії, а її автор заслуговує на присудження йому ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки та інформаційні технології».

Офіційний опонент
Професор спецкафедри
Академії зовнішньої розвідки України
доктор технічних наук, професор Людмила КОВАЛЬЧУК

30.08.2021

ПОГОДЖЕНО
Проректор з наукової роботи
Академії зовнішньої розвідки України
кандидат наук з державного управління Володимир КОЛЕСНИК

30.08.2021