# ВІДГУК

офіційного опонента
професора кафедри електроніки Національного авіаційного університету
доктора технічних наук, професора Білецького Анатолія Яковича
на дисертаційну роботу Лади Наталії Володимирівни
«Метод синтезу операцій потокового шифрування з точністю до перестановки», подану на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – Системи захисту інформації

Цей відгук підготовлено за матеріалами дисертації, що містить основний текст роботи на 160 сторінках, додатками до дисертації, актами впровадження наукових результатів, авторефератом на 20 сторінках і копіями 16 наукових праць здобувача.

**Актуальність теми дисертації.** У зв'язку з безперервно зростаючим обсягом інформації, що циркулює в різноманітних системах передачі повідомлень, різко збільшуються вимоги, що пред'являються, по-перше, як до швидкості обміну даними, так і, по-друге, простоті апаратно-програмної реалізації систем, які здійснюють прийом-передачу повідомлень, і, нарешті, по-третє, надійності захисту таких систем від несанкціонованого доступу до конфіденційної інформації.

Далеко не повний наведений перелік вимог, що пред'являються до сучасних електронних систем передачі цифрових даних, диктує необхідність переходу до малоресурсних засобів (і алгоритмів) криптографічного захисту інформації (LWC - Lightweight Cryptography), що забезпечують, з одного боку, високі швидкості передачі повідомлень, що досягаються, як правило, в системах потокового шифрування, а з іншого — порівняно незначний обсяг апаратно-програмних засобів, що потрібен для реалізації LWC технологій. Особливої актуальності малоресурсна криптографія набуває в останні роки, для яких характерне масове впровадження в повсякденну практику Інтернет речей (IoT), що найбільш ефективно забезпечують безпеку мережевих структур різного типу.

Чи не максимально можлива швидкість криптографічних перетворень вихідної інформації (в умовах малоресурсних запитів на забезпечення необхідного захисту і приймо-передачу даних) досягається при використанні алгоритмів і засобів поточного шифрування, теорія і практика якого далека від завершення. Якраз розробці нових підходів і методів поточного шифрування, орієнтованих на застосування оригінальних перестановок вхід-вихідних даних, і присвячено дане дослідження.

Дисертаційна робота виконана відповідно до Постанови Президії НАНУ від 20.12.13 №179 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2014–2018 рр.», а саме – пп. 1.2.8.1. «Розробка методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії», а також Постанови КМУ від 7 вересня 2011 року №942 «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2020 року», а саме – «Технології та засоби захисту інформації». Результати дисертаційної роботи включені в НДР «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах» (ДР № 0115U003103), «Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування» (ДР № 0112U003579), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР № 0116U008714), «Методи та засоби захисту конфіденційних даних в хмарних сховищах» (ДР №0116U008713), «Розробка методів та засобів оцінки ефективності соціоінжинірингу» (ДР № 0116U008715), в яких автор брав участь як виконавець.

Тому вважаю, що тема дисертаційного дослідження «Метод синтезу операцій потокового шифрування з точністю до перестановки», та вирішена у роботі наукова задача підвищення якості криптографічного захисту інформації на основі застосування нових потокових шифрів є *актуальною*.

**2. Наукова новизна результатів роботи**

У роботі досліджено підвищення якості функціонування систем криптографічного захисту інформаційних ресурсів за рахунок розробки та застосування оригінальних потокових шифрів з використанням криптографічних примітивів заснованих на перестановках.

До основних нових наукових результатів, отриманих в дисертації, на мою думку, слід віднести наступні.

1) уперше розроблено метод синтезу модифікованих операцій додавання за модулем два з точністю до перестановки на основі експериментальних досліджень шляхом поєднання матричних криптоалгоритмів з перестановками операндів і результатів виконання операцій, що забезпечило побудову симетричних та несиметричних модифікованих операцій, визначення і формалізацію взаємозв'язків між

операціями та алгоритмами для прямого і оберненого перетворення інформації;

2) удосконалено метод синтезу повної групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки операндів, що забезпечило можливість синтезу математичних моделей криптографічного перетворення та побудову уніфікованого пристрою шифрування на її основі;

3) отримало подальший розвиток метод підвищення стійкості та надійності потокового шифрування на основі застосування групи модифікованих операцій додавання за модулем два з точністю до перестановки шляхом використання додаткової гамуючої послідовності для вибору операцій на кожному етапі шифрування, що забезпечило підвищення якості шифрування та виключило можливість витоку інформації і ускладнило відтворення гамуючої послідовності зловмисником при однократних відмовах в системі.

**3. Достовірність наукових результатів**

Достовірність основних наукових результатів роботи підтверджується наведеною в розділах 2, 3 і 4 коректною системою формальних методик і перетворень, рядом наведених прикладів та їх графічною інтерпретацією, результатами комп'ютерного моделювання і впровадженням отриманих результатів та розроблених засобів.

**4. Цінність дисертаційної роботи для науки**

Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної задачі в теорії побудови швидкодіючих криптографічних засобів для захисту інформації з підвищеною стійкістю і надійністю шифрування. Змістовний аспект запропонованого рішення, який спрямований на підвищення якості функціонування систем потокового шифрування шляхом застосування отриманої групи модифікованих операцій додавання за модулем два з точністю до перестановки і запропонованих засобів для їх реалізації, не був відомий раніше.

**5. Практична корисність роботи**

Практична корисність роботи обумовлена тим, що використання запропонованих в ній формальних методів і конкретних рішень дозволяє отримувати більш досконалі, порівняно з відомими, засоби криптографічного потокового шифрування. Результати роботи впроваджено на підприємствах та в навчальний процес деяких університетів.

## 6. Структура роботи

Дисертаційна робота містить вступ, 4 розділи, висновки, додатки та перелік використаних джерел.

**У вступі** сформульовано актуальність теми роботи, мету і задачі дослідження, наукову новизну і практичне значення отриманих результатів, показано зв‘язок роботи з науковими програмами, планами і темами, виконуваними у Черкаському державному технологічному університеті, наведено відомості про реалізацію і апробацію роботи, про публікації за її темою.

**У першому розділі** наведено обґрунтування необхідності вдосконалення систем захисту інформації. Проведено стислий огляд поширених криптографічних систем, здійснено аналіз основних операцій, на основі яких будуються системи криптографічного захисту інформації. Запропоновано гіпотезу про можливість підвищення якості потокового шифрування за рахунок модифікації операції додавання за модулем два. Сформульовано мету та задачі наукового дослідження.

**Другий розділ** присвячений синтезу і аналізу симетричних та несиметричних модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки операндів.

**Третій розділ** присвячено синтезу та дослідженню повної групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки результатів виконання операцій. Запропоновано метод синтезу та технологію дослідження операцій додавання за модулем два з точністю до перестановки результатів виконання операції.

**Четвертий розділ** присвячено синтезу і дослідженню оберненого криптографічного перетворення з використанням операцій додавання за модулем два з точністю до перестановки результатів виконання операції. Розроблено метод підвищення стійкості та надійності потокового шифрування на основі застосування синтезованої групи модифікованих операцій та оцінці якості його використання.

**У додатках** подано результати моделювання операцій потокового шифрування, результати статистичного дослідження результатів шифрування, акти про впровадження результатів дисертаційного дослідження, а також обов’язкову інформацію про публікацію та апробацію результатів дослідження.

## 7. Публікації за темою дисертації

Наукові положення дисертації, що пов’язані з підвищенням якості

систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та надійності перетворення на основі використання модифікованих операцій додавання за модулем два з точністю до перестановки достатньо повно відображені в публікаціях автора і пройшли апробацію на міжнародних науково-технічних конференціях і семінарах.

**8. Автореферат дисертації**

Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі.

**9. Зауваження щодо змісту дисертаційної роботи та автореферату**

1. В підрозділі 1.1 «Актуальність захисту інформації в інформаційно-телекомунікаційних системах» на ст. 14-17 автор наводить перелік нормативно-правових документів у сфері захисту інформації, який в подальшому не використовується.

2. Підрозділ 1.2 «Сучасний стан розвитку комп'ютерної криптографії» переповнений загальновідомою інформацією та класифікаціями систем криптографічного захисту інформації. Доцільно було б дану інформацію навести в вигляді таблиць і схем, та приділити більше уваги, висвітленню переваг та недоліків окремих крипто примітивів, на основі яких і базуються всі подальші дослідження.

3. Припущення, приведене на ст. 34, про достатність дослідження лише 6 операцій (по одній з кожної комутативної групи), на мою думку є некоректним, тому що при дослідженні несиметричних операцій необхідно досліджувати всі модифікації в групі, що і робить автор в підрозділі 2.2. «Аналіз груп операцій, синтезованих на основі додавання ...».

4. На мою думку, недостатньо описані взаємозв'язки між циклами крипто перетворень в орієнтованому псевдографі криптоперетворень на основі матричних алгоритмів (рис 2.5), а результати аналізу псевдографа подані лише таблично, що значно ускладнило сприйняття результатів аналізу орієнтованого псевдографу крипто перетворень та узагальненої схеми циклів взаємного перетворення наведених в підрозділі 4.2. В авторефераті опис даних взаємозв'язків відсутній.

5. Відсутність в матеріалах дисертації методики, на основі якої проводився синтез універсальної схеми реалізації групи операцій додавання за модулем два з точністю до перестановки (рис. 4.10), зменшує практичне значення отриманих результатів для синтезу дискретних пристроїв спеціального призначення.

6. Взаємозв'язки між модифікованими операціями криптографічного додавання за модулем два з точністю до перестановки і кодами команд управління універсальною схемою реалізації групи операцій для прямого і

оберненого криптоперетворення наведені у табл.4.18., без обґрунтування та додаткових пояснень. Не зрозуміло, чому саме таку таблицю взаємозв'язків взято автором для реалізації потокового шифрування, з декількох можливих варіантів її побудови, а також не наведено даних про можливість застосування інших наборів команд для керування універсальною схемою реалізації групи операцій додавання.

7. При оцінці ефективності отриманих результатів, було б доцільно детально розглянути особливості застосування апарату мінімізації недетермінованих кінечних автоматів для оцінки якості шифрування, а не обмежитися посиланнями на опубліковані результати досліджень.

8. В роботі і авторефераті присутні стилістичні та орфографічні неточності.

**10. Загальна оцінка дисертації**

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-технічної задачі, спрямованої на підвищення якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та надійності перетворення на основі використання модифікованих операцій додавання за модулем два з точністю до перестановки. Дисертація є завершеною науково-дослідною роботою. Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота задовольняє вимогам "Порядку присудження наукових ступенів", а її автор Лада Наталія Володимирівна заслуговує присудження наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – системи захисту інформації.

Офіційний опонент
професор кафедри електроніки
Національного авіаційного університету,
заслужений діяч науки і техніки України,
лауреат Державної премії України,
д.т.н., професор А. Я. Білецький

15.01.2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ * Ідентифікаційний код 01132330 * М. КИЇВ *

Підпис Білецького А.Я.
засвідчую
Вчений секретар
Національного авіаційного університету
Г. Єгорова