ВІДГУК

офіційного опонента – завідувача кафедри біофізики, інформатики та медапаратури Вінницького національного медичного університету ім. М.І. Пирогова, доктора технічних наук, професора Кулика Анатолія Ярославовича

на дисертаційну роботу **Козловської Світлани Григорівни** *«Методи синтезу груп симетричних операцій для потокового шифрування»*, що подана на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.05 – Комп'ютерні системи і компоненти

Актуальність теми дисертації.

На сьогоднішній день криптографічний захист інформації є одним із найефективніших засобів забезпечення інформаційної безпеки як окремих фірм, так і держав в цілому. Невпинність технічного прогресу вимагає створення нових та вдосконалення існуючих методів та засобів криптографічного захисту. Дедалі більше уваги для вирішення цієї задачі приділяють розширенню кількості операцій, придатних для прямого та оберненого криптоперетворення інформації. Для уникнення некоректності та помилок під час застосування нових операцій вони потребують детального дослідження.

Розвиток потокових шифрів пов'язаний з вирішенням задач генерації високоякісних псевдовипадкових послідовностей та побудови нових логічних операцій потокового шифрування. Одним з перспективних напрямів розвитку потокового шифрування є застосування булевих функцій для побудови операцій криптоперетворення інформації. Разом з тим, задачі синтезу груп симетричних двохоперандних операцій потокового шифрування не було розглянуто.

Дисертаційна робота виконувалась відповідно до плану наукових досліджень Черкаського державного технологічного університету. Напрямки досліджень дисертаційної роботи пов'язані з реалізацією Постанови Президії НАНУ від 25.02.2009 р. № 55 «Про основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009 - 2013 рр.» (п. 1.2.7.1. Розробка методів та інформаційних

технологій розв'язання задач комп'ютерної криптографії та стеганографії; п. 1.2.7.2. Розробка методів підвищення продуктивності систем асиметричної криптографії), 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 – п. 1.2.8.1. «Розробка методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії», а також Постанови КМУ від 7 вересня 2014 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 дисертаційних досліджень були використані:

- при виконанні науково-дослідної роботи «Метод синтезу швидкодіючих систем захисту інформації на основі спеціалізованих логічних функцій» (ДР № 0108U000506);
- в науково-дослідній роботі «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР № 0116U008714);
- в науково-дослідній роботі «Метод синтезу механізмів захисту інформації в спеціалізованих автоматизованих системах» (ДР № 0108U000508).

В зв'язку з вищевикладеним тема даної роботи, спрямованої на розроблення методів синтезу груп симетричних операцій для потокового шифрування, безперечно є актуальною.

Загальна оцінка змісту дисертаційної роботи.

У вступі в повній мірі здобувачем аргументовано вибір теми дисертаційного дослідження, розкрито актуальність, сформульовано мету, для реалізації якої коректно поставлені відповідні завдання, визначено об'єкт, предмет, методи, наукову новизну та практичне значення досліджень.

Перший розділ присвячено розгляду сучасного стану та перспектив розвитку методів синтезу та аналізу операцій криптографічного перетворення для захисту конфіденційної інформації. Показано, що сьогодні криптографія залишається

основним засобом захисту конфіденційної інформації. Розглянуто класифікації криптографічних методів та проаналізовано шляхи розвитку комп'ютерної криптографії.

Визначено, що одним із перспективних напрямів розвитку систем криптографічного захисту інформації є використання операцій криптографічного перетворення на основі логічних функцій. Розглянуто сучасний стан досліджень операцій криптографічного перетворення інформації з акцентуванням на особливостях застосування в потоковому та блочному шифруваннях. Проведений аналіз дозволив виявити сукупність недоліків, що властиві традиційним підходам до побудови криптосистем даного класу, обґрунтувати науково-прикладну задачу, визначити перспективний напрям досліджень і сформулювати задачі дисертаційної роботи.

У *другому розділі* розглянуто питання математичного моделювання та дослідження двохоперандних операцій криптографічного перетворення інформації на основі відомих таблиць істинності.

Для забезпечення ефективності проведення досліджень проаналізовано та класифіковано таблиці істинності симетричних дворозрядних двооперандних операцій криптоперетворення. Кожна з наведених двооперандних операцій є операцією вибору однієї з чотирьох однооперандних операцій перетворення першого операнда (x_1, x_2) залежно від значення другого операнда (y_1, y_2), який виконує функцію команд управління ($y_1 = k_1, y_2 = k_2$). Послідовність однооперандних операцій для їхнього вибору представлено послідовністю індексів операції. Взаємозв'язок індексів двооперандної операції з моделями однооперандних операцій зведено до таблиці.

На основі унікальності наборів однооперандних операцій наведено операції, розбиті на 24 набори двооперандних операцій (НДО) по чотири операції в кожному наборі. Всім наборам двохоперандних операцій присвоєно порядковий номер. Крім того, всі операції поділено на чотири математичні групи.

На основі аналізу отриманих результатів побудовано узагальнені перестановочні схеми для першої математичної групи двооперандних операцій криптоперетворення.

Третій розділ висвітлює питання дослідження другої математичної групи двооперандних операцій криптоперетворення.

Дослідження проведено шляхом застосування методу побудови і дослідження двооперандних операцій криптоперетворення на основі результатів обчислювального експерименту.

В процесі дослідження перестановочних схем таблиць істинності встановлено, що:

- сукупність наборів таблиць істинності двооперандних операцій криптоперетворення другої математичної групи створюють повну групу наборів таблиць істинності двооперандних операцій криптоперетворення;
- групи перестановочних схем першої та другої математичної групи досліджених операцій криптоперетворення співпадають;
- підтверджене припущення про те, що застосування повної групи перестановочних схем забезпечить побудову повної групи наборів двооперандних операцій криптоперетворення невідомої групи та їх таблиць підстановки, якщо взяти будь-яку операцію з цієї невідомої групи.

У *четвертому розділі* здійснюється синтез груп двооперандних операцій криптоперетворення та оцінювання ефективності їхнього застосування. Після узагальнення результату дослідження моделей операцій першої групи отримано класифікацію операцій з поділом на базові операції, поєднання базових операцій з операціями перестановки та поєднання базових операцій з операціями перестановки та інверсії.

Проведені дослідження стали основою для розроблення методу синтезу груп дворозрядних двооперандних операцій для симетричного потокового шифрування. Оскільки основною операцією цієї групи є операція додавання за модулем два, то й групу було названо симетричною групою двооперандних дворозрядних операцій криптографічного додавання за модулем два.

За аналогією з цим методом розроблено також метод синтезу симетричної групи двооперандних дворозрядних операцій криптографічного додавання за модулем чотири, оскільки основною операцією другої групи є операція додавання за модулем чотири.

Наведені результати статистичних досліджень практичних результатів дисертаційної роботи свідчать, що досліджувані послідовності пройшли комплексний контроль за методикою випробувань пакетом тестів NIST_STS.

Обгрунтованість висновків і одержаних результатів дисертаційної роботи базується на коректному використанні вихідних посилань і математичного апарату теорій інформації, ймовірності, алгоритмів, криптографії із застосуванням методів дискретної математики, комп'ютерного моделювання та математичної статистики.

Вірогідність результатів дисертаційної роботи підтверджується імітаційним комп'ютерним моделюванням, яке показало коректність теоретичних досліджень та ефективність розроблених методів і засобів, їх експериментальною перевіркою, що підтверджуються відповідними актами впроваджень.

Найбільш вагомими науковими результатами, отриманими в дисертації є:

- вперше розроблений метод побудови та дослідження двооперандних операцій криптоперетворення на основі результатів обчислювального експерименту шляхом формалізації, класифікації і математичного перетворення, що забезпечило встановлення нових взаємозв'язків між операндами і результатами, а також можливість застосування однооперандних операцій у потоковому шифруванні;
- вперше розроблені методи синтезу груп симетричних дворозрядних двооперандних операцій потокового шифрування на основі результатів обчислювального експерименту шляхом застосування результатів реалізації розробленого методу побудови та дослідження двооперандних операцій і табличного представлення класифікації групи однооперандних двохрозрядних операцій криптографічного перетворення, а також встановлення нових раніше невідомих взаємозв'язків між однооперандними та двооперандними операціями, що

забезпечило синтез математичних груп симетричних двооперандних операцій на основі додавання за модулем два та за модулем чотири;

- удосконалення методу підвищення стійкості та надійності потокового шифрування на основі додаткового застосування синтезованих груп симетричних двооперандних операцій криптографічного перетворення інформації, що забезпечило підвищення стійкості та варіативності потокового шифрування.

Практична цінність отриманих результатів полягає в тому, що отримані наукові результати доведено здобувачем до конкретних інженерних методик та варіантів функціональних схем спеціалізованих дискретних пристроїв, які реалізують криптографічне перетворення інформації на основі застосування синтезованих груп операцій потокового шифрування та забезпечують підвищення варіативності й стійкості до лінійного криптоаналізу.

На підставі проведених досліджень одержано такі практичні результати: алгоритми функціонування та функціональні схеми реалізації груп операцій криптографічного додавання за модулем два та модулем чотири, що дало можливість підвищити якість систем потокового й блокового шифрувань інформації.

Результати дисертаційної роботи впроваджені і пройшли апробацію у Центральному конструкторському бюро «Сокіл» Науково-виробничого комплексу «ФОТОПРИЛАД» (м. Черкаси) під час проектування спеціалізованого модуля операційної системи. Також результати дисертаційної роботи використовувались у навчальному процесі Черкаського державного технологічного університету на кафедрі інформаційної безпеки та комп'ютерної інженерії в матеріалах лекційних курсів «Основи криптографічного захисту інформації», «Комп'ютерні методи та засоби захисту інформації».

Рекомендації щодо використання наукових результатів.

Теоретичні положення, отримані в роботі, можуть бути розповсюджені на комп'ютерні системи різного функціонального призначення, як для закриття збереженої інформації, так і для її передавання.

Додаткового дослідження вимагають алгоритми реалізації для спеціалі-

зованих комп'ютерних систем.

Завершеність, стиль виконання, публікації.

Аналіз сукупності наукових результатів, поданих в роботі Козловської С.Г. дозволяє зробити висновок про їх цілісність і засвідчує особистий внесок автора в науку щодо розроблення комп'ютерних компонентів для забезпечення необхідно рівня захисту даних.

Всього за тематикою дисертації опубліковано 12 друкованих праць, в тому числі: п'яти статтях в наукових журналах і збірниках наукових праць, внесених до списку українських та закордонних фахових видань; одній колективній монографії; шести тезах доповідей на міжнародних науково-технічних та науково-практичних конференціях.

Головні наукові результати дисертації повністю опубліковано і відображено у зазначених працях.

Матеріали досліджень обговорювались на 6 науково-технічних конференціях різного рівня.

Зміст автореферату повністю відповідає основним положенням і висновкам, зробленим в дисертації.

Зміст дисертації відповідає паспорту спеціальності 05.13.05 – Комп'ютерні системи і компоненти.

Недоліки та зауваження по роботі:

1. Метою дослідження є «підвищення якості систем…», але що під цим розуміється не пояснюється.
2. Апробація результатів досліджень лише на конференціях в м. Черкаси, а на тих де не місто є співорганізатором.
3. В переліку праць не вказано скільки з опублікованих входять до наукометричних баз.
4. Розділ 1 має суто описовий характер без будь-яких доказових розрахунків.

5. Наведене у розділі 2 припущення не містить обґрунтувань та обмежень, що не є строгим твердженням.
6. Розділи 2 та 3 містять елементи системного аналізу, але про це ніде не згадується.
7. Термін «синтез» є набагато ширшим, ніж це подано в роботі. Доцільніше було б говорити про «розроблення».
8. У наведених схемах не виділені процесори та інші комп'ютерні компоненти, хоча розробка явно призначена для комп'ютерних систем.
9. Рисунки на стор. 134, 135 малоінформативні і вимагають додаткових пояснень.
10. В роботі декларується «підвищення стійкості та надійності», але методика їх розрахунку не наведена, а таблиця 4.4 такої інформації не надає.
11. У висновках до розділу 4 декларується «збільшення варіативності потокового шифрування в 5 раз», але звідки взята ця цифра незрозуміло.
12. В роботі говориться про обчислювальний експеримент, але його методика та умови проведення не обґрунтовані.
13. В роботі зустрічаються термінологічні, стилістичні та орфографічні помилки.

Висновок.

Незважаючи на вказані зауваження загальна оцінка дисертаційної роботи позитивна. Вони не знижують цінності отриманих наукових та практичних результатів. Дисертаційна робота Козловської С.Г. виконана на високому науковому рівні, є завершеною науковою працею, яка має суттєве практичне значення та спрямована на розв'язання актуальної науково-технічної задачі. Дисертаційна робота «Методи синтезу груп симетричних операцій для потокового шифрування» відповідає вимогам пп. 9, 11, 12 "Порядку присудження наукових ступенів", затвердженому постановою Кабінету Міністрів України № 567 від 24 липня 2013 р. та паспорту спеціальності. Автор дисертації Козловська Світлана Григорівна заслуговує на присвоєння їй наукового ступеня ка-

ндидата технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи і компоненти.

Зав. кафедри біофізики, інформатики
та медапаратури Вінницького національного
медичного університету ім. М.І. Пирогова,
д.т.н., професор Кулик А.Я.

Міністерство охорони здоров'я України
Вінницький національний медичний університет ім. М.І. Пирогова
Ідент. код 02010669

Підпис Кулика А.Я.
завіряю
ст. інсп. відділу кадрів
Вінницького національного
медичного університету
ім. М. І. Пирогова
(Л.О. Тарнова)
«12» 06 20 19 р.