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 **Нестеренко Оксани Борисівни**
«Методи та засоби синтезу операцій потокового шифрування
за критерієм строгого стійкого кодування»,
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 проблема захисту інформаціїстала принципово важливою для Державної служби України з надзвичайних ситуацій. Особливо велике значення має оперативність, достовірність і конфіденційність інформації для управління підрозділами в кризових ситуаціях, адже від них залежить безпека та життя людей.

За останні десятиліття значно зросла кількість робіт, пов'язаних із криптографією та криптоаналізом, які опубліковані у відкритих наукових виданнях. Накопичений значний теоретичний і практичний потенціал використовується не тільки для побудови, а і для злому криптосистем. Не зважаючи на всі ризики, криптографія на сьогоднішній день залишається найбільш ефективним і поширеним засобом інформації у кіберпросторі. Підтвердженням важливості розвитку криптографії є конкурси на стандарти криптографії, які постійно проводять як у нашій державі, так і в світі.

Створення квантових комп'ютерів та стрімке збільшення хмарних сховищ вимагають застосування високовидкісної потокової комп'ютерної криптографії, яка забезпечить максимальну невизначеність результатів шифрування.

Дисертаційна робота виконувалась відповідно до плану наукових досліджень Черкаського державного технологічного університету. Напрямки досліджень дисертаційної роботи пов'язані з реалізацією 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»; Постанови Президії НАНУ від 30.01.2019 №30 «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019–2023 роки», а саме – п. 1.2.8.1 «Розроблення методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії»; 1.2.8.2 «Розроблення методів підвищення продуктивності систем асиметричної криптографії».

Результати дисертаційних досліджень були використані:

- при виконанні науково-дослідної роботи «Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування» (ДР № 0112U003579);
- в науково-дослідній роботі «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР№ 0116U008714).

В зв'язку з вищевикладеним тема даної роботи, спрямованої на розроблення методів та засобів операцій потокового шифрування за критерієм строгого стійкого кодування, 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 аналізу якості систем криптографічного перетворення інформації. Обґрунтовується актуальність і необхідність проведення аналізу якості криптографічних систем. Проводиться огляд сучасних вимог до криптографічних систем та вибираються вимоги, які доцільно ви-

користовувати в даному дисертаційному дослідженні. Для подальшого дослідження проводиться аналіз відомих досліджень стосовно лавинного ефекту, який оцінюється критерієм строгого лавинного ефекту (СЛК). Детально аналізуються властивості лавинного ефекту та критерії їх оцінки. Проводиться огляд наукових досліджень стосовно надійності та безпеки криптографічних систем. Аналізуються підходи до оцінки стійкості криптографічних алгоритмів. Розглядаються атаки на криптоалгоритми, уточнюються особливості атак на асиметричну криптосистему. Розглядаються аспекти і чинники надійності криптосистем. 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 дослідженню двохрозрядних операцій криптографічного перетворення інформації за критерієм строгого стійкого криптографічного кодування.

Проведене дослідження дворозрядних елементарних функцій для криптоперетворення на відповідність СЛК показало, що жодна з елементарних функцій, на основі яких будуються всі 24 операції криптоперетворення, не відповідають вимогам критерію, бо не забезпечують зміну половини бітів інформації на повній множині вхідних даних.

Оскільки елементарні функції криптоперетворення не відповідають вимогам СЛК, то і всі операції, які будуються з даних елементарних функцій, також не відповідають вимогам даного критерію.

Для оцінки якості операцій криптоперетворення було запропоновано, по аналогії зі СЛК, ввести критерій строгого стійкого кодування (ССК). Криптографічний алгоритм, або операція криптографічного перетворення інформації задовольняє ССК, якщо незалежно від ключової послідовності та вхідної інформації кожний біт вихідної послідовності змінюється відносно вхідної інформації з імовірністю одна друга. Подальші дослідження показа-

ли, що лише 4 двохрозрядні операції з 24 відповідають ССК.

Встановлено, якщо в дворозрядних операціях інвертується один з переставлених бітів, то перестановка буде «плаваючою», а отже, біт буде інвертуватися і визначатися не тільки інверсією розряду в операції, а й вхідною інформацією. Відзначений факт показує можливість створення потокових шифрів, у яких результат побітового шифрування залежить не тільки від значення бітів гамуючої послідовності, а й від значення бітів даних, які шифруються.

В основу подальших досліджень було покладено гіпотезу про те що, при якісному шифруванні немає необхідності виконувати повторне шифрування.

Третій розділ висвітлює питання розроблення методу синтезу операцій криптографічного перетворення інформації за критерієм строгого стійкого криптографічного кодування.

Запропоновано етапи побудови 4 двохоперандних операцій, які досліджено: будується таблиця відстаней за Хеммінгом; видаляються з таблиці значення відстаней всі, крім одиниці; замінивши в кожному рядку однакові значення відстаней, що залишилися, значенням рядка, отримаємо проміжну таблицю вибору варіантів підстановки; видаливши зсувом пусті клітинки, отримаємо таблицю вибору варіантів підстановки; послідовним вибором у кожному стовпчику результату шифрування значення першого рядка, не допускаючи повторів, отримаємо варіанти таблиць підстановок операцій ССК.

У *четвертому розділі* здійснюється розроблення методу синтезу операцій криптографічного перетворення інформації та оцінка можливості застосування синтезованих операцій у потоковому шифруванні.

В процесі аналізу синтезованих і досліджених моделей операцій, які відповідають ССК, було відмічено, що складність моделей відрізняється, а моделі операцій, які мають найменшу складність, складаються лише з перестановок і інверсій. Узявши це припущення за основу моделювання опера-

цій, було отримано 42 чотирьохрозрядні операції.

На основі отриманих результатів було сформульовано метод синтезу операцій криптографічного перетворення інформації мінімальної складності за критерієм ССК. Сутність цього методу полягає в наступному: синтез операцій, які задовольняють критерію ССК і мають мінімальну складність, проводиться на основі парних перестановок та інверсії шляхом інверсії половини бітів, за умови однієї інверсії в кожній парній перестановці.

Удосконалення методів синтезу програмно-апаратних засобів комп'ютерної криптографії полягає в побудові операцій криптоперетворення мінімальної складності без виконання етапів синтезу таблиць істинності та етапу мінімізації логічних функцій.

Проте для ефективного застосування в потокових шифрах синтезовані операції повинні одночасно обробляти два операнди, один з яких – інформація, другий – псевдовипадкова послідовність.

Обгрунтованість висновків і одержаних результатів дисертаційної роботи базується на коректному використанні вихідних посилань і математичного апарату теорії інформації, теорії алгоритмів, теорії множин, криптографії, математичної логіки, теорії графів, методів дискретної математики, математичної статистики та комп'ютерного моделювання.

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 синтезу операцій за критерієм строгого стійкого

кодування шляхом використання таблиць мінімальних відстаней за Хеммінгом для побудови таблиць істинності дискретних моделей, які забезпечують максимальну невизначеність результатів перетворення та збільшення варіативності криптоалгоритмів;

- вперше розроблений метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності на основі використання операцій перестановки і гамування, шляхом встановлених обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при практично мінімальній складності схемотехнічної та програмної реалізації.

Практична цінність отриманих результатів полягає в тому, що отримані наукові результати доведено здобувачем до конкретних інженерних методик та варіантів функціональних схем функціональних схем і програмних модулів для реалізації операцій потокового шифрування, які гарантовано забезпечують зміну кожного біта інформації з імовірністю одна друга.

Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS. Крім того, застосування цих послідовностей в імовірнісних моделях на прикладі інтегральної моделі розвитку і припинення пожежі забезпечило підвищення точності моделювання.

Результати дисертаційної роботи впроваджені і пройшли апробацію у приватному підприємстві «Сенсорна Електроніка» (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 спеціалізовані комп'ютерні системи як для закриття збереженої інформації, так і для її передавання.

Додаткового дослідження вимагають алгоритми реалізації для комп'ютерних систем різного функціонального призначення.

Завершеність, стиль виконання, публікації.

Аналіз сукупності наукових результатів, поданих в роботі Нестеренко О.Б. 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 у 18 друкованих працях, в тому числі: 7 статтях у наукових журналах і збірниках наукових праць, внесених до списку фахових видань України; 1 одноосібній статті в закордонному науковому виданні; 1 колективній монографії; 9 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 9 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. Розділ 1 має суто описовий характер без будь-яких доказових розрахунків.
2. В розділі 2 вказано, що кодування побітове, але якщо потрібно передавати блоками в режимі реального часу, то як це впливатиме на шифратор? В роботі цього не показано.

3. В роботі відсутні розрахунки швидкодії, що ускладнює використання алгоритмів в режимі реального часу.
4. На стор. 69 вказано, що використовується четвіркова система числення, хоча в роботах Шеннона доведено, що оптимальною є експоненціальна..
5. В роботі велика увага приділена плануванню експерименту, хоча ніде про це не згадується.
6. Алгоритм не може базуватися на словах типу «нехай» (стор. 71), оскільки це викликає невизначеність.
7. В роботі не розглядаються і не використовуються класичні методи рандомізації, які давно алгоритмізовані.
8. У наведених схемах не виділені процесори та інші комп'ютерні компоненти, хоча розробка явно призначена для комп'ютерних систем.
9. В роботі використовується формула Бернуллі. Але на її використання накладаються певні обмеження, про які не згадується.
10. В дисертації не показано за яких умов доцільно використовувати апаратну, програмну чи комбіновану реалізацію.
11. В роботі говориться про комп'ютерне моделювання, але його методика та умови здійснення не обґрунтовані.
12. 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 Нестеренко О.Б. 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 та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування» відповідає вимогам пп. 9, 11, 12 "Порядку присудження наукових ступенів", затвердженому постановою Ка-

бінету Міністрів України № 567 від 24 липня 2013 р. та паспорту спеціальності. Автор дисертації Нестеренко Оксана Борисівна заслуговує на присвоєння їй наукового ступеня кандидата 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
відділу кадрів
Вінницького національного
медичного університету
ім. М. І. Пирогова
«12» 06 2019 р.