Ученому секретарю
спеціалізованої вченої ради
Д 26.062.17
при Національному авіаційному
університеті

03058, м. Київ,
просп. Космонавта Комарова, 1

ВІДГУК

офіційного опонента, професора кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна доктора технічних наук, професора Кузнецова Олександра Олександровича на дисертацію Гришакова Сергія Володимировича «Метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – «Інформаційна безпека держави».

1. Актуальність теми дисертації

Відповідно до основних положень українських нормативно-правових актів під інформаційною безпекою держави розуміють стан її інформаційної захищеності, при якій випадки зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації (за допомогою спеціальних технічних засобів) та комп'ютерні злочини не завдають суттєвої шкоди національним інтересам. Стрімкий розвиток сучасних комп'ютерних технологій, їх поширення та запровадження, окрім надання новітніх інформаційних послуг, зумовлює також і поширення нових викликів та загроз інформаційній безпеці. В умовах глобальної світової інтеграції та жорсткої міжнародної конкуренції інформаційний простір стає головним місцем зіткнень та кібернетичної протидії. Особливу небезпеку в цьому розумінні становлять сучасні загрози інформаційної та кібербезпеки державним інформаційним ресурсам та технологіям, інформаційним, телекомунікаційним та інформаційно-телекомунікаційним системам, що використовуються задля збереження військової та державної таємниці, персональних даних та іншої інформації, вимоги щодо захисту якої встановлені законом.

Важливим механізмом криптографічного захисту інформації є потокове симетричне шифрування, яке забезпечує підвищені показники швидкодії та стійкості до нав'язування хибних режимів функціонування кінцевого обладнання. Саме тому потокові шифри найбільш часто використовують для захисту інформаційних державних ресурсів, зокрема, в телекомунікаційних системах спеціального призначення. Отже аналіз, дослідження та подальший

розвиток потокових шифрів є безумовно важливим та актуальним напрямком досліджень, який тісно пов'язаний із виконанням сучасних вимог та умов, визначених Стратегією кібербезпеки України (затвердженою Указом Президента України від 15 березня 2016 року № 96), Доктриною інформаційної безпеки України (затвердженою Указом Президента України від 25 лютого 2017 року № 47/2017) на іншими нормативно-правовими актами України.

Одним із перспективних напрямків розвитку потокового шифрування є застосування методів випадкового кодування та нелінійних відображень. Проте стійкість відомих рандомізованих шифросистем вивчена недостатньо, досі не обґрунтовані практичні схеми та рекомендації щодо їх застосування у різних криптографічних додатках. Отже, тема дисертаційної роботи є актуальною, вибір напрямку наукових досліджень є обґрунтованим.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації

2.1. У першому розділі дисертаційної роботи автором проводиться аналіз ефективності побудови та реалізації рандомізованих шифросистем, що використовуються в спеціальних інформаційно-телекомунікаційних системах. Зокрема, досліджено роль та практичне значення рандомізованих потокових шифросистем у забезпеченні безпеки державних інформаційних ресурсів, наведено класифікацію шифросистем, досліджено їх математичні моделі, показники стійкості та ефективності, тощо. За результатами аналізу відомих методів побудови рандомізованих симетричних блокових та потокових шифросистем зроблено висновок про складність їх реалізації, малопрактичність конструкцій та відсутності оцінок стійкості відносно відомих криптоаналітичних атак. Далі автором розглянуто системи передачі інформації каналом зв'язку з відводом та рандомізовані потокові шифросистеми Міхалевича-Імаї, сформульовано протиріччя, на розв'язання якого спрямовано мету дисертаційного дослідження. Зокрема, відзначено потребу в обчислювально стійких та практичних рандомізованих потокових шифросистемах, що необхідні для забезпечення безпеки державних інформаційних ресурсів, з одного боку, та відсутністю розвинутих методів їх побудови з іншого. Розділ закінчується формулюванням мети, об'єкту, предмету, наукового завдання та основних напрямків (часткових задач) дисертаційного дослідження, висновками по першому розділу дисертації.

В цілому слід зазначити, що цей розділ містить обґрунтовані результати аналізу та аналітичного огляду різних варіантів побудови рандомізованих шифросистем, що свідчить про високу кваліфікацію здобувача, його ерудицію в обраній предметній області та фахову підготовку. Однак слід зазначити наступні **недоліки та зауваження:**

- підрозділ 1.2 присвячено класифікації, математичним моделям, показникам стійкості та ефективності рандомізованих симетричних шифросистем. Основним показником ефективності визначено

швидкість передачі інформації, а показник стійкості визначено в теоретико-інформаційному розумінні через ненадійність повідомлення та ключа. Однак далі за текстом ці показники стійкості жодного разу не застосовуються, ненадійність не розраховується, а стійкість завжди оцінюється тільки в обчислювальному вимірюванні через кількість операцій, які необхідно виконати для пошуку секретного ключа;

- при описі відомих методів побудови рандомізованих шифросистем бракує посилань. Зокрема, у п. 1.3.1 при описі методів 1.1-1.6 (с. 30-35) та у п. 1.3.2 при описі методів 2.1-2.3 (с. 38-41) автор посилається лише на одне джерело, опубліковане понад 35 років назад;
- у змісті назва п. 1.3.3 із помилкою, зокрема замість «… з відводом» помилково вказано «… з відомим».

2.2. Другий розділ дисертації присвячено дослідженню обчислювальної стійкості та практичності рандомізованих потокових шифросистем Міхалевича-Імаї. Зокрема, у розділі наведено формальне означення та основні показники ефективності шифросистем, досліджено їх обчислювальну стійкість відносно атак на основі відомих шифрованих повідомлень, на основі підібраних відкритих повідомлень та на основі підібраних векторів ініціалізації. За результатами проведених досліджень зроблено висновки про залежність обчислювальної стійкості від вибору окремих параметрів кодів та генератору гами. В цьому розділі автором також було отримано аналітичні межі для швидкості передачі інформації при заданих обмеженнях відносно стійкості та ймовірності правильного прийому повідомлень.

Отримані результати подано, переважно, у вигляді лем та математичних тверджень із відповідним доведенням. Змістовна частина розділу насичена логічними виведеннями, математичними формулами та аналітичними міркуваннями, за допомогою яких автором встановлюється істинність певних суджень та гіпотез. Це свідчить про підготовленість здобувача до професійної дослідницької діяльності, його спроможність самостійно формулювати та вирішувати складні наукові та практичні задачі.

Недоліки, зауваження та пропозиції за другим розділом дисертації:

- на рис. 2.1 наведено схему рандомізованої потокової шифросистеми Міхалевича-Імаї. Але замість формального подання каналу передачі даних із певними спотвореннями на рисунку вказано блок моделювання. Отже, це не схема шифросистеми, а схема її моделі. Інакше схему треба виправити та подати, наприклад, як на рис. 3.1 у розділі 3;
- у п. 2.2.1 та 2.2.2 досліджено обчислювальну стійкість потокової шифросистеми Міхалевича-Імаї до атак на основі відомих шифрованих повідомлень та до атаки на основі підібраних відкритих повідомлень, відповідно. Але конкретних оцінок стійкості не наведено (як це зроблено у п. 2.2.3 при дослідженні стійкості відносно атаки на основі підібраних векторів ініціалізації), наведено лише констатацію можливості

проведення таких атак та вказано задачі (розв'язання системи рівнянь), які для цього треба вирішити;

- у підрозділі 2.3 наведено аналітичні межі для швидкості передачі інформації в шифросистемі Міхалевича-Імаї із зауваженням про достатність умов існування шуканих об'єктів без зазначення ефективного способу їх побудови. Доцільним, на мій погляд, було б навести конкретні значення для відомих прикладів з побудови цих шифросистем, порівняти їх із отриманими аналітичними межами та прокоментувати з погляду перспектив подальших досліджень, пошуку кращих альтернатив. Зокрема, цікаво, як співвідносяться реальні приклади із залежностями, які наведено на рис. 2.4 (залежності верхніх оцінок швидкості передачі інформації).

2.3. Третій розділ дисертації «Метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням» присвячено формальному означенню та дослідженню обчислювальної стійкості рандомізованих потокових шифросистем. Зокрема, автором досліджується обчислювальна стійкість відносно атак на основі відомих шифрованих повідомлень та на основі підібраних векторів ініціалізації в різних випадках застосування. Ці дослідження проводилися стосовно запропонованого автором альтернативного методу побудови шифросистем, сутність якого полягає в застосуванні для випадкового кодування нелінійних відображень або безключових геш-функцій. Отримані наукові результати встановлюють умови обчислювальної стійкості запропонованих шифросистем відносно відомих атак та свідчать про глибоке розуміння автором сутності вирішуваних завдань, їх важливості для теорії та практики створення рандомізованих перетворень як альтернативного напрямку побудови сучасних симетричних криптоалгоритмів.

До недоліків (або краще до суб'єктивних рекомендацій) за цим розділом слід віднести наступне:

- основним науковим результатом цього розділу, а, можливо, й всієї роботи, є запропонований метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням, сутність якого полягає в застосуванні для випадкового кодування нелінійних відображень або безключевих геш-функцій. На жаль, у тексті дисертації бракує детального опису запропонованого методу із наведенням всіх обчислювальних процедур та функцій, вимогами та умовами практичної реалізації, обґрунтованими рекомендаціями для застосування у різних криптографічних додатках. Це полегшило б сприйняття запропонованої ідеї інженерами-практиками, дозволило б прискорити імплементацію нових технічних рішень та перевірити на практиці їх коректність та відтворюваність. Сутність свого методу автор викладає в одному реченні, лише кількома фразами встановлюючи відмінні ознаки. Далі зосереджується на абстрактних математичних виразах та уявленнях, які потрібні йому для розв'язання математичних завдань оцінки

обчислювальної складності. Тобто автор зовсім не приділяє увагу інженерним питанням реалізації запропонованого методу, а зосереджується виключно на цікавих для нього речах – теоретичному обґрунтуванні стійкості абстрактних математичних конструкцій. В результаті нова ідея, новий метод побудови шифросистеми виглядає другорядним, хоча саме він буде практично застосований і саме від його використання буде отримано практичну користь. Оскільки дисертація висувається за технічними науками акцент роботи, як на мене, зроблено невірно;

- у продовження попереднього недоліку слід відмітити відсутність патентного захисту запропонованого методу. Якщо це нова ідея (а з огляду на результати проведеного аналізу так воно і є), тоді необхідно негайно захистити авторські та майнові права на нову розробку, шляхом, наприклад, отримання авторського свідоцтва на твір, патенту на корисну модель або винахід, тощо.

2.4. У четвертому розділі дисертації «Результати порівняння стійкості та ефективності програмних реалізацій рандомізованих потокових шифросистем» автором проводяться порівняння запропонованих шифросистем з шифросистемами Міхалевича-Імаї за стійкістю та швидкістю передачі, обґрунтовується вибір компонент для побудови, зокрема, нелінійних відображень, генераторів гами, випадкових послідовностей, тощо. Наводяться результати дослідження ефективності програмних реалізацій запропонованих шифросистем з нелінійним випадковим кодуванням.

Цей розділ, фактично, містить короткий огляд криптографічних примітивів, які можна застосувати у якості складових запропонованої шифросистеми. Спрощену структуру шифросистеми можна подати у вигляді трьох основних компонентів: генератор випадкових чисел, нелінійне відображення та генератор гами. Автор розглядає різні варіанти побудови кожного компонента та пропонує три реалізації, які згодом і досліджує.

Недоліки та зауваження за четвертим розділом дисертації:

- загалом автор обґрунтовано робить вибір найбільш досліджених та відомих геш-функцій Keccak та «Кипина» (національні стандарти США та України) у якості механізмів реалізації нелінійного відображення та генератору ключового потоку SNOW 2.0 (алгоритм з міжнародного стандарту) у якості генератору гами. Але не зрозуміло, чому автором зосереджено увагу лише на генераторі випадкових послідовностей ISAAC (Indirection, Shift, Accumulate, Add and Count), чому не розглянуті інші варіанти;
- порівняння за швидкістю шифрування та розшифрування носять однобокий характер та не є цілком об'єктивними. Зокрема, автор порівнює запропоновані варіанти між собою та з відомим блоковим шифром AES (національний стандарт США). Предметом дослідження є

методи побудови потокових шифросистем, але автор уникає порівняння саме з сучасними потоковими алгоритмами;
- інколи у тексті трапляються незрозумілі термінологічні звороти, наприклад: «моделювати генератор випадкових послідовностей за допомогою генератора псевдовипадкових чисел» (с. 130), «криптографічна схема варіанту реалізації шифросистеми» (с. 132), тощо.

2.5. У висновках акцентується увага на науковій задачі дисертаційного дослідження, методах її вирішення. Сформульовано наукові результати, вказано на їх достовірність, значимість для теорії та практики, наведено рекомендації щодо використання отриманих результатів.

3. Достовірність отриманих результатів

Достовірність результатів дисертаційної роботи підтверджується збіжністю отриманих результатів експериментальних досліджень шляхом імітаційного та комп'ютерного моделювання з теоретичними результатами та аналітичними співвідношеннями. Достовірність отриманих результатів обґрунтовується їх несуперечністю основним положенням математичного апарату теорії складності алгоритмів, теорії чисел, теорії груп, полів, кілець, прикладної криптології, методів математичного та комп'ютерного моделювання, теорії ймовірностей та математичної статистики. Слід відмітити також адекватність припущень, які лежать в основі проведених наукових досліджень, а також коректне застосування відомих математичних методів, що також опосередковано підтверджує достовірність отриманих результатів.

4. Новизна отриманих результатів

У дисертаційній роботі Гришакова С.В. «Метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням» отримано теоретичне узагальнення та нове вирішення актуальної науково-прикладної задачі, яка полягає в розробці методу побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням для забезпечення безпеки державних інформаційних ресурсів.

Отримано такі **науково обґрунтовані результати**.
- вперше отримано аналітичні оцінки параметрів, що визначають стійкість шифросистеми Міхалевича-Імаї відносно атак на основі відомих шифрованих повідомлень, а також підібраних векторів ініціалізації;
- вперше доведено, що клас шифросистем Міхалевича-Імаї володіє суттєвою слабкістю, яка полягає в зменшенні кількості інформації, що необхідна для відновлення за реальний час символів відкритого тексту;
- вперше отримано аналітичні межі для швидкості передачі інформації в шифросистемі Міхалевича-Імаї при заданих обмеженнях щодо

ймовірності правильного прийому повідомлень законним користувачем та стійкості шифрування;

- отримав подальший розвиток метод побудови рандомізованих потокових шифросистем, який базується на застосуванні для випадкового кодування нелінійних відображень або безключових геш-функцій.

5. Завершеність, стиль викладення, публікації

5.1. Аналіз сукупності наукових результатів і положень, характеристику яких наведено в пп. 2-4, дозволяє зробити висновок про їх внутрішню єдність і засвідчує особистий внесок автора у науку. У дисертаційній роботі отримано розвиток методів побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням для забезпечення безпеки державних інформаційних ресурсів.

5.2. Дисертація є завершеною науковою роботою, виконаною і оформленою відповідно до встановлених вимог.

5.3. Дисертаційна робота написана зрозуміло і грамотно, науково-технічна термінологія використовується коректно, структура роботи логічна.

5.4. Основні результати досліджень опубліковані досить повно в 15 наукових працях: з них 8 наукових статей в наукових спеціалізованих виданнях України та інших країн (4 видання індексуються міжнародними наукометричними базами), 7 тез доповідей на наукових та науково-практичних конференціях.

5.5. Структура і зміст автореферату повністю відповідає тексту дисертації.

6. Практична значимість

6.1. В дисертаційній роботі розроблено спеціальне програмне та математичне забезпечення з реалізації рандомізованих потокових шифросистем з нелінійним випадковим кодуванням на основі нелінійних відображень та безключових геш-функцій. Розроблені реалізації дозволяють здійснювати процедури зашифровування та розшифровування даних і можуть бути використані у якості прототипу для спеціальних додатків, витоки конфіденційної інформації в яких створюють ризики для інформаційної безпеки держави.

6.2. Отримані наукові та практичні результати дисертаційної роботи реалізовані в Службі зовнішньої розвідки України, зокрема в результаті виконання НДР «Кета» (акт від 14.09.2016) та в науково-технічних розробках ПАТ «Інститут інформаційних технологій» (акт від 25.07.2016).

7. Недоліки та зауваження

Основні недоліки, зауваження та пропозиції викладено при аналізі наукових результатів дисертанта (п.2), однак вони не впливають на загальний позитивний висновок про дисертаційну роботу.

8. Загальні висновки

8.1. Дисертація є закінченою науково-дослідною роботою, яка містить теоретичне узагальнення та нове рішення актуальної науково-прикладної задачі, яка полягає в розробці методу побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням для забезпечення безпеки державних інформаційних ресурсів.

8.2. Зміст дисертації відповідає паспорту спеціальності 21.05.01 – «Інформаційна безпека держави».

8.3. Дисертаційна робота Гришакова С.В. «Метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням» має певну наукову новизну і практичну значимість у галузі безпеки інформаційних технологій, відповідає вимогам п. 9-14 "Порядку присудження наукових ступенів", а її автор заслуговує присудження наукового ступеня кандидата технічних наук.

Професор кафедри безпеки інформаційних систем і технологій
Харківського національного університету імені В.Н. Каразіна
доктор технічних наук, професор О.О. КУЗНЕЦОВ

"12" 09 2018 р.

Підпис доктора технічних наук,
професора КУЗНЕЦОВА О.О. засвідчую

Учений секретар Н.А. Вінтякова

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В.Н. КАРАЗІНА * ХАРКІВ * 02071205