Голові спеціалізованої вченої
ради Д 26.062.17
Національного авіаційного університету
03058, м. Київ, проспект
Космонавта Комарова, 1

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

на дисертацію Гришакова Сергія Володимировича
«Метод побудови рандомізованих потокових шифросистем з
нелінійним випадковим кодуванням»,
прийнятої до захисту на здобуття наукового ступеня кандидата технічних наук за
спеціальністю 21.05.01 – інформаційна безпека держави

Актуальність. Зростання рівня зовнішніх загроз національній безпеці України надає особливої важливості задачам забезпечення інформаційної безпеки держави. Одним із основних напрямків вирішення цих задач є створення нових та удосконалення існуючих методів криптографічного захисту інформації. Реалізації криптосистем повинні бути швидкими та криптографічно стійкими до всіх відомих криптоаналітичних атак. Особливо це стосується спеціальних (військових) додатків, в яких широко використовуються потокові шифри. Оскільки швидка заміна алгоритму шифрування, криптографічні слабкості якого виявлені на етапі його експлуатації, є практично неможливою, видається доцільним створення методів підвищення стійкості потокових шифрів без внесення змін в алгоритми шифрування шляхом застосування додаткових перетворень, які не потребують ключів, можуть бути відносно просто реалізовані та забезпечують науково обґрунтований рівень стійкості систем шифрування в цілому.

Тому, робота Гришакова Сергія Володимировича «Метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням», що спрямована на підвищення криптографічної стійкості потокових шифрів шляхом рандомізації джерела відкритих повідомлень для забезпечення безпеки державних інформаційних ресурсів є безумовно актуальною.

Зв'язок роботи з науковими програмами, планами та темами.

Дисертаційне дослідження проводилося відповідно до планів науково-дослідної роботи Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» та в межах науково-дослідної роботи «Кета» (номер держреєстрації 0114U004643) на замовлення Служби зовнішньої розвідки України.

Оцінка змісту дисертації, її завершеності у цілому.

Робота складається із анотації, змісту, переліку умовних позначень, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел (в кінці кожного розділу). Загальний обсяг дисертації – 214 сторінок, з них 127 сторінок основного тексту, які включають 30 рисунків, 3 таблиці.

У **вступі** автором представлена загальна характеристика роботи, обґрунтована актуальність наукової теми, сформульовані мета та задачі, відображено наукову новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо їх апробації та впровадження.

Перший розділ роботи присвячено аналізу відомих методів побудови рандомізованих симетричних шифросистем та їх практичному значенню у забезпеченні безпеки державних інформаційних ресурсів. Показано, що більшість відомих методів рандомізації зводяться до певних варіантів лінійного випадкового кодування та наступного зашифровування відкритих повідомлень. Крім того, відомі методи побудови рандомізованих блокових шифросистем з нелінійним випадковим кодуванням не можуть бути безпосередньо застосовані для побудови рандомізованих потокових шифросистем через специфіку атак саме на потокові шифри. Показано, що єдиним відомим прикладом рандомізованих потокових шифросистем, які можуть бути використані на практиці, є шифросистеми Міхалевича-Імаї. Рандомізатори цих шифросистем будуються на основі двійкових лінійних перетворень, зокрема, завадостійкого кодування відкритих повідомлень лінійними кодами. Проте стійкість шифросистем Міхалевича-Імаї суттєво залежить від будови їх компонент і може бути значно меншою, ніж стверджують їх розробники. Деякі з цих шифросистем виявляються вразливими навіть до атак на основі відомих шифрованих повідомлень і, отже, не можуть бути використані для захисту державних інформаційних ресурсів.

У **другому розділі** запропоновано атаки на рандомізовані потокові шифросистеми Міхалевича-Імаї на основі відомих шифрованих повідомлень, а також підібраних векторів ініціалізації. Ці атаки дозволяють отримувати інформацію про ключ, а в окремих випадках відновлювати ключ цілком.

Важливим науковим результатом розділу є загальний теоретично обґрунтований факт, що клас рандомізованих потокових шифросистем Міхалевича-Імаї (незалежно від будови їх компонент) володіє суттєвою слабкістю, яка полягає в зменшенні кількості інформації (в порівнянні з довжиною блоку шифрувальної гами), необхідної для відновлення за реальний час символів відкритого тексту. Зазначена властивість є наслідком спільного застосування випадкового і завадостійкого кодування повідомлень лінійними кодами та непритаманна аналогічним за будовою шифросистемам, де випадкове кодування не використовується.

У розділі, також отримані аналітичні межі для швидкості передачі інформації в рандомізованих потокових шифросистемах Міхалевича-Імаї, що

дозволяють з'ясувати їх потенційні можливості та визначити загальні обмеження, яким задовольняють окремі показники їх ефективності при заданих значеннях інших показників.

У **третьому розділі** викладено альтернативний метод побудови рандомізованих потокових шифросистем з підвищеною стійкістю, сутність якого полягає в застосуванні для випадкового кодування нелінійних відображень або безключевих геш-функцій. На відміну від раніше відомих, запропонований метод надає більше можливостей для побудови обчислювально стійких шифросистем за рахунок розширення класу перетворень, що використовуються в конструкції рандомізатора.

У розділі, також отримано аналітичні оцінки параметрів, що характеризують обчислювальну стійкість запропонованих шифросистем відносно атак, подібних тим, які будуються для шифросистем Міхалевича-Імаї. Наслідком отриманих результатів є встановлені вимоги до нелінійного відображення.

Четвертий розділ присвячено порівнянням запропонованих шифросистем з шифросистемами Міхалевича-Імаї за стійкістю та швидкістю передачі при однаковій довжині шифрованих повідомлень. Крім того, розроблено програмні реалізації трьох варіантів рандомізованих потокових шифросистем з нелінійним випадковим кодуванням, що дозволяють здійснювати на практиці процедури зашифровування/розшифровування даних в режимі реального часу (програмний код вказаних реалізацій наведено в додатках).

З метою оцінки на практиці ефективності рандомізованих потокових шифросистем з нелінійним випадковим кодуванням розроблено та програмно реалізовано конкретні варіанти шифросистем. Показано, що побудовані рандомізовані потокові шифросистеми можуть бути застосовані на практиці для зашифровування/розшифровування даних в режимі реального часу.

У загальних **висновках** викладено найбільш важливі наукові та практичні результати, отримані у дисертаційній роботі, які дають розв'язок сформульованих задач дисертаційного дослідження.

Список використаних джерел, що наведений в кожному розділі є інформативним, достатньо повно охоплює предметну галузь, відображає опрацювання здобувачем значної кількості іноземних джерел.

В цілому викладення отриманих наукових і практичних результатів є послідовним, логічним та обґрунтованим, експериментальна частина не суперечить теоретичній, а дисертаційне дослідження має завершений характер.

Вміст автореферату достатньо повно розкриває основні положення дисертації та відповідає вимогам до оформлення.

Повнота викладу в опублікованих працях.

Матеріали дисертаційної роботи достатньо повно опубліковані в восьми статтях, що опубліковані в наукових спеціалізованих виданнях України та інших

країн (чотири видання індексуються міжнародними наукометричними базами), а також у семи матеріалах конференцій. Проведено апробацію і обговорення результатів дослідження на семи міжнародних наукових конференціях.

Обсяг друкованих робіт та їх кількість відповідає вимогам щодо публікації основного змісту дисертації на здобуття наукового ступеня кандидата технічних наук.

Найбільш суттєві наукові результати дисертації:

1. Отримано аналітичні оцінки параметрів, що визначають стійкість рандомізованих потокових шифросистем Міхалевича-Імаї відносно атак на основі відомих шифрованих повідомлень, а також підібраних векторів ініціалізації. Отримані оцінки дозволяють з'ясувати теоретико-кодовий сенс параметрів, які визначають обчислювальну стійкість цих шифросистем, а також встановити, що стійкість таких шифросистем може бути значно меншою, ніж стверджують їх розробники.

2. Доведено, що клас рандомізованих потокових шифросистем Міхалевича-Імаї володіє суттєвою слабкістю, яка полягає в зменшенні кількості інформації, що необхідна для відновлення символів відкритого тексту за реальний час. Зазначена властивість дозволяє зробити практично важливий висновок про те, що для відновлення символів відкритого тексту супротивнику достатньо мати лише часткову інформацію про секретний ключ рандомзованих потокових шифросистем.

3. Отримано аналітичні межі для швидкості передачі інформації в рандомізованих потокових шифросистемах Міхалевича-Імаї при заданих обмеженнях щодо ймовірності правильного прийому повідомлень законним користувачем та стійкості шифрування. Зазначені межі, за рахунок застосування оцінок Плоткіна та Бассалиго-Елайєса для швидкості передачі лінійних кодів, дозволяють зробити науково обґрунтований висновок про обмеження можливості рандомізованих потокових шифросистем Міхалевича-Імаї з погляду сучасних вимог щодо стійкості та практичності в реальних умовах.

4. Розвинуто метод побудови рандомізованих потокових шифросистем, який базується на застосуванні для випадкового кодування нелінійних відображень або безключових геш-функцій та дозволяє збільшити стійкість в порівнянні з рандомізованими потоковими шифросистемами Міхалевича-Імаї за рахунок розширення класу перетворень, що використовуються в конструкції рандомізатора.

Ступінь обґрунтованості та достовірності наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Ступінь обґрунтованості наукових положень, висновків та рекомендацій у дисертації обумовлена коректністю застосування математичних методів

оцінювання обчислювальної стійкості рандомізованих потокових шифросистем. Для аналізу існуючих методів побудови рандомізованих шифросистем, а також розробки методу побудови шифросистем з нелінійним випадковим кодуванням застосовувались методи лінійної алгебри, теорії ймовірностей та теорії інформації. Дослідження стійкості шифросистем Міхалевича-Імаї та шифросистем з нелінійним випадковим кодуванням здійснювалось з використанням методів лінійної алгебри, теорії ймовірностей, математичної статистики, а також теорії складності обчислень. При побудові аналітичних меж для швидкості передачі інформації в шифросистемах Міхалевича-Імаї застосовувались методи теорії кодування.

Достовірність та обґрунтованість підтверджені всебічною апробацією на багатьох наукових та науково-практичних конференціях, наявністю рецензованих спеціалістами публікацій у фахових виданнях, впровадженням розроблених методів у держбюджетних науково-дослідних роботах.

Практичне значення отриманих результатів та можливі шляхи їх використання.

Практична цінність роботи полягає в тому, що розроблений автором метод побудови рандомізованих потокових шифросистем може застосовуватися у спеціальних (військових) додатках для побудови шифросистем з нелінійним випадковим кодуванням на основі нелінійних відображень або безключевих геш-функцій, що є більш стійкими (у 2^{242} і більше разів) і більш швидкісними (у 125 і більше разів) за шифросистеми Міхалевича-Імаї при однаковій довжині вхідного повідомлення.

Практична цінність роботи підтверджена впровадженням її результатів у науково-дослідній роботі «Кета» (акт від 14.09.2016), а також в науково-технічних розробках ЗАО «Інститут інформаційних технологій» (акт від 25.07.2016).

Дискусійні положення, недоліки, зауваження та побажання. У цілому, позитивно оцінюючи роботу, слід звернути увагу на окремі положення дисертаційної роботи, що мають дискусійний характер чи потребують додаткового обґрунтування або пояснень. Суть основних з них полягає в такому:

1. Другий розділ роботи присвячено докладному аналізу обчислювальної стійкості рандомізованих потокових шифросистем Міхалевича-Імаї відносно різноманітних атак. Так у розділі для зменшення складності кодування в шифросистемі Міхалевича-Імаї матриці G_1 і G_2 задаються відповідно формулі 2.4. Цікаво, якщо матриці G_1 і G_2 задати за іншими правилами, чи всі наведенні у розділі твердження будуть виконуватись.

2. У четвертому розділі роботи автор досліджує ефективність рандомізованих потокових шифросистем з нелінійним випадковим кодуванням, де в якості

генератора гами обирає лише криптографічний алгоритм SNOW 2.0, в якості відображення ϕ – дві геш-функції "Купину" та Keccak та одне нелінійне відображення, а в якості генератора випадкових послідовностей – один алгоритм ISAAC. На мою думку, було б доцільно дослідити ефективність запропонованих автором шифросистем при більшій кількості обраних генераторів гами та генераторів випадкових послідовностей.

3. У табл. 4.3 роботи наводиться час виконання процедур зашифровування/розшифровування для рандомізованих потокових шифросистем з нелінійним випадковим кодуванням та алгоритму AES. Але із роботи не зрозуміло чи дані, що наведені у таблиці отримані з одного експерименту, чи це усередненні значення серії експериментів. Тому, складно у повній мірі оцінити отримані результати. Крім того, біло б цікаво побачити як змінюється час виконання процедур зашифровування/розшифровування при збільшенні розміру досліджуваних файлів (наприклад, при розмірі файлу 1 ГБ) та при використанні різних обчислювальних систем. Також, було б доцільно програмно реалізувати декілька варіантів шифросистеми Міхалевича-Імаї та провести аналогічні дослідження часу виконання процедур зашифровування/розшифровування та експериментально підтвердити підвищення швидкодії рандомізованих потокових шифросистем з нелінійним випадковим кодуванням над шифросистемами Міхалевича-Імаї.

4. По тексту дисертації є незначні орфографічні помилки. Деякі рисунки наводяться з недостатніми поясненнями, що ускладнює їх сприйняття. На рис. 2.1, де відображена схема рандомізованої потокової шифросистеми Міхалевича-Імаї в передавачі відсутня операція складання за модулем 2 вектора v_i з гамою $f_i(k)$ та результатом випадкового і завадостійкого кодування повідомлення s_i $((s_i,u_i)G_2G_1 \oplus f_i(k)$, $i=0,1,...,t)$.

5. В дисертації наводиться велика кількість тверджень, проте не для всіх із них є доведення, що ускладнює їх аналіз. Наприклад, твердження 2.3, 3.4 та 3.5.

При цьому, слід відмітити, що наведені зауваження та недоліки не є принциповими щодо вирішення науково-практичного завдання, не впливають на загальне позитивне враження від роботи, не зменшують наукової цінності та практичності.

Загальні висновки.

У цілому дисертаційна робота Гришакова С.В. «Метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням» є завершеною, самостійно підготованою кваліфікаційною працею, в якій на підставі теоретичних та експериментальних досліджень надано нове вирішення важливої наукової задачі, щодо розробки методу побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням для забезпечення безпеки державних інформаційних ресурсів.

Дисертаційна робота містить не захищені раніше наукові положення та нові результати, спрямовані на розвиток та вдосконалення криптографічних методів захисту. Сформульовані наукові положення, висновки та рекомендації є достовірними та обґрунтованими. Матеріал дисертації викладено логічно і послідовно, стиль викладання чіткий і зрозумілий. Висновки до розділів та до дисертації в цілому тісно пов'язані з їх змістом і відображають основну суть роботи. Зміст автореферату повністю відповідає тексту дисертації, а основні наукові положення, які в них містяться, є ідентичними. Наукові положення та висновки досить повно відображені в фахових виданнях. Матеріали дисертації достатньою мірою апробовані на міжнародних конференціях.

Дисертаційна робота відповідає профілю спеціалізованої вченої ради Д 26.062.17 та паспорту спеціальності 21.05.01 – інформаційна безпека держави.

Таким чином, за своєю актуальністю, ступенем достовірності та обґрунтованості наукових положень, висновків, новизною, практичним значенням і повнотою викладу в опублікованих працях дисертаційна робота «Метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням» відповідає вимогам до кандидатських дисертацій, а її автор, Гришаков Сергій Володимирович, заслуговує на присудження наукового ступеня кандидата технічних наук зі спеціальності 21.05.01 – інформаційна безпека держави.

ОФІЦІЙНИЙ ОПОНЕНТ
Кандидат технічних наук,
доцент кафедри
безпеки інформаційних технологій
Навчально-наукового інституту
інформаційно-діагностичних систем
Національного авіаційного університету **В.М. Кінзерявий**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ 01132330 * МІСТО КИЇВ *

Підпис Кінзерявого В.М.
засвідчую
Вчений секретар
Національного авіаційного університету
Г. Сичева