ВІДГУК

офіційного опонента на дисертаційну роботу

ФАУРЕ ЕМІЛЯ ВІТАЛІЙОВИЧА

«Методологія захисту інформації на основі факторіального кодування даних»,

подану на здобуття наукового ступеня

доктора технічних наук за спеціальністю

05.13.21 – системи захисту інформації

1. Актуальність теми. Інформаційно-телекомунікаційні системи та мережі використовуються на сьогодні для передавання даних різноманітного призначення, в тому числі з обмеженим доступом. Несанкціоноване втручання в роботу таких систем може призводити до негативних наслідків, пов’язаних зі значними матеріальними втратами, невиконанню завдань в умовах військових дій тощо. Серед можливих загроз під час передавання та зберігання інформації в телекомунікаційних системах є: несанкціоноване читання інформації з обмеженим доступом, несанкціонована модифікація (підміна) інформації, пошкодження інформації внаслідок дії природних завад у каналі зв’язку. На сьогодні кожна з перелічених загроз блокується окремими методами та алгоритмами обробки інформації. Застосування окремих процедур призводить до ускладнення структури системи, збільшення навантаження на обчислювальні пристрої, зменшення їх швидкодії, збільшення введеної надлишковості та, як наслідок, зменшення відносної пропускної здатності каналу зв’язку. Тому представляється досить актуальним розроблення та дослідження таких методів, які дозволяють в рамках одного алгоритму обробки інформації з введенням мінімальної надлишковості вирішувати декілька задач її захисту.

Таким чином, поставлена у дисертаційній роботі Фауре Еміля Віталійовича проблема розробки методології захисту інформації на основі факторіального кодування даних для побудови систем захисту інформації від несанкціонованого доступу та помилок у каналі зв’язку із забезпеченням підвищення достовірності передавання інформації є актуальною на сучасному етапі розвитку науки та техніки.

2. Ступінь обґрунтованості наукових положень дисертації, їх достовірність і новизна. Основні наукові результати дослідження, висновки та рекомендації чітко сформульовані, достатньо обґрунтовані та не викликають сумнівів. Достовірність наукових положень дисертації забезпечується коректним використанням теорії захисту інформації, завадостійкого кодування,

факторіального числення, теорії ймовірностей та математичної статистики, статистичного аналізу.

Основні наукові результати дисертації, на мій погляд, полягають у наступному:

вперше:

- розроблено методи роздільного факторіального кодування інформації, які за рахунок реалізації єдиної процедури завадостійкого кодування та захисту від нав'язування хибних даних шляхом використання перестановки в якості перевірної частини кодового слова дозволяють забезпечити контроль цілісності інформації та підвищити її достовірність при передаванні в телекомунікаційних системах;
- розроблено методи нероздільного факторіального кодування інформації, які за рахунок реалізації єдиної процедури завадостійкого кодування та шифрування шляхом бієктивного перетворення інформаційної послідовності в перестановку чисел заданого порядку, параметри якого тримаються в таємниці, дозволяють забезпечити захист інформації від помилок у каналі зв'язку та несанкціонованого доступу, а також підвищити її достовірність під час передавання;
- розроблено математичну модель процесу декодування факторіальних кодів, яка за рахунок дослідження механізмів перетворення одного кодового слова в інше в симетричному двійковому каналі з незалежними бітовими помилками дозволяє оцінити показники достовірності передавання інформації в результаті застосування факторіального кодування та підтвердити його переваги порівняно з іншими методами завадостійкого кодування;
- теоретично обґрунтовано принципи побудови комбінаційного генератора, що дозволило сформувати загальні вимоги до первинних послідовностей і комбінаційної функції для забезпечення необхідних статистичних властивостей послідовності чисел, зокрема, в реалізаціях запропонованого методу формування перестановок на основі факторіальної системи числення;
- розроблено метод оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, який за рахунок дослідження закону розподілу знаків емпіричної автокореляційної функції відносно кількості символів в перекритих частинах відрізків, на які розбивається послідовність чисел, і визначення допустимого «порогу» перекриття, нижче якого спостерігається рівномірний розподіл знаків автокореляційної функції, дозволяє виявити статистичні властивості, що є притаманними послідовностям, породженим природними джерелами дискретного білого шуму, і не є притаманними штучно згенерованим псевдовипадковим послідовностям (ПВП);

удосконалено:

– метод формування випадкової послідовності перестановок на основі використання факторіальної системи числення, який за рахунок введення додаткового генератора випадкових чисел (ГВЧ) дозволяє зменшити обсяг внутрішньої пам'яті додаткового ГВЧ не менш ніж на кількість біт, що дорівнює двійковому логарифму від порядку генерованих перестановок, уникнути порушення рівномірності їх розподілу та підвищити швидкість їх формування;

- метод формування ПВП на основі лінійного конгруентного методу, який дозволяє формувати ПВП рівномірно розподілених чисел максимального періоду незалежно від топології графа станів лінійного конгруентного генератора (ЛКГ), зменшити часові витрати на вибір параметрів ЛКГ та збільшити розмір простору їх допустимих значень для досягнення максимального періоду в число разів, що дорівнює відношенню потужності алфавіту ЛКГ до її функції Ейлера;

- метод криптографічного захисту інформації на основі операції гамування, який за рахунок введення другого контуру шифрування та використання в ньому принципів конкатенації зв'язних компонентів у графі станів ЛКГ дозволяє зменшити ймовірність зламу шифру методом повного перебору ключового простору та підвищити стійкість до статистичного криптоаналізу.

Сукупність указаних вище принципів і методів формують методологію захисту інформації на основі факторіального кодування даних, яка за рахунок формалізованого механізму використання розроблених методів і моделей роздільного та нероздільного факторіального кодування, а також методів і моделей формування ключових послідовностей для факторіального кодування дозволяє створювати системи інтегрованого захисту інформації від помилок у каналі зв'язку та несанкціонованого перехоплення або несанкціонованої модифікації.

3. Практична цінність результатів полягає, в першу чергу, у розроблених структурних схемах та алгоритмах роботи пристроїв кодування та декодування факторіальних кодів, пристроїв формування послідовностей перестановок, пристрою криптографічного перетворення даних, розроблених критеріях і методиках перевірки послідовностей рівномірно розподілених випадкових чисел.

Додатково практична цінність дисертаційного дослідження підтверджується актами впровадження в ДП «НДІ «Акорд» (система дистанційного зв'язку, контролю та управління віддаленими об'єктами, м. Черкаси), ТОВ «Діджитал Мастер» (імітатор модуля керування метеорологічним локатором «Буран-А» авіаційного тренажера КТС-148, м. Київ), Департамент освіти та гуманітарної політики Черкаської міської ради (система обліку кадрів, м. Черкаси), а також у

навчальний процес Черкаського державного технологічного університету, Черкаського інституту пожежної безпеки імені Героїв Чорнобиля та Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут».

4. Оцінка змісту та структури дисертаційної роботи. Дисертаційна робота складається зі вступу, шести розділів, висновків, додатків і списку використаних джерел (355 найменувань). Повний об’єм дисертації складає 477 сторінок, у тому числі 312 сторінок основного тексту.

У вступі обґрунтовано актуальність дослідження, наведено зв’язок роботи з науковими програмами, планами та темами, визначено мету та задачі роботи, визначено об’єкт та предмет дослідження. Наведено наукову новизну та практичну цінність отриманих результатів, визначено особистий внесок здобувача в роботах, опублікованих у співавторстві, представлено відомості про апробацію та публікації результатів дослідження.

У першому розділі проведено огляд існуючих підходів, методів і засобів сумісного захисту інформації від помилок у каналі зв’язку, несанкціонованого доступу, модифікації даних, а також методів формування й оцінювання генераторів випадкових чисел. Визначено напрямки та основні задачі дослідження.

У другому розділі удосконалено метод формування випадкової послідовності перестановок на основі використання факторіальної системи числення, розроблено структурну схему та алгоритм роботи пристрою формування випадкової послідовності перестановок; розроблено принципи та методи роздільного факторіального кодування інформації, а також структурні схеми та алгоритми роботи пристроїв кодування та декодування роздільних факторіальних кодів; розроблено математичну модель процесу декодування роздільних факторіальних кодів.

У третьому розділі розроблено принципи та методи нероздільного факторіального кодування інформації, структурні схеми та алгоритми роботи пристроїв кодування та декодування нероздільних факторіальних кодів; розроблено математичну модель процесу декодування нероздільних факторіальних кодів.

У четвертому розділі розроблено модель узагальненого графа станів лінійного конгруентного генератора; удосконалено метод формування псевдовипадкової послідовності на основі лінійного конгруентного методу, розроблено структурну схему та алгоритм роботи пристрою формування псевдовипадкової послідовності перестановок на основі лінійного конгруентного генератора з будь-яким типом графа його станів; удосконалено метод симетричного

криптографічного захисту інформації на основі операції гамування, розроблено структурну схему та алгоритм роботи пристрою двоконтурного криптографічного перетворення даних.

У п'ятому розділі теоретично обґрунтовано принципи побудови комбінаційного генератора з комбінаційною функцією підсумовування за модулем слів, отриманих від групи первинних генераторів рівномірно розподілених випадкових чисел як з необмеженими, так і з обмеженими періодами, а також перестановок, які циклічно повторюються; розроблено методику вибору параметрів первинних генераторів перестановок для дослідженого комбінаційного генератора.

У шостому розділі розроблено метод оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел; розроблено та реалізовано критерії і методики тестування послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел; розроблено методологію захисту інформації на основі факторіального кодування даних, яка дозволяє забезпечити підтримку процесів створення систем інтегрованого захисту інформації від помилок у каналі зв'язку та несанкціонованого доступу.

Додатки містять допоміжний матеріал з результатів досліджень, а також 6 актів впровадження результатів роботи.

5. Повнота викладу наукових положень, висновків, рекомендацій в опублікованих працях здобувача. Основні наукові результати, що отримані в дисертації, у повній мірі викладені здобувачем у 80 наукових працях, основні 60 з яких наведено в авторефераті. У тому числі: 2 розділи в колективних монографіях, 4 наукові статті у виданнях, що індексуються наукометричними базами Scopus / Web of Science, 2 наукові статті у фахових виданнях інших країн та 27 статей у наукових виданнях, що входять до переліку МОН України та індексуються іншими наукометричними базами, 12 патентів України та 13 матеріалів і тез доповідей наукових конференцій.

Апробацію результатів досліджень на міжнародних та всеукраїнських науково-технічних конференціях слід визнати достатньою.

6. Відповідність дисертації встановленим вимогам. Дисертація написана сучасною науково-технічною мовою, її оформлення відповідає вимогам МОН України, що пред'являються до дисертаційних робіт. Зміст автореферату достатньо повно розкриває зміст дисертації, об'єктивно відображає основні положення дисертаційної роботи.

У цілому можна позитивно оцінити дисертаційне дослідження, відзначити його наукову новизну та практичне значення, високий теоретичний рівень.

7. Відповідність паспорту спеціальності. Основні результати роботи спрямовані на створення систем захисту інформації від помилок у каналі зв'язку, несанкціонованої модифікації та несанкціонованого доступу до інформації й відповідають паспорту спеціальності 05.13.21 – системи захисту інформації, зокрема, п. 1 «Теоретичні, методологічні, технічні, технологічні й організаційні основи створення комплексних систем захисту інформації (СЗІ), зокрема інформації, що зберігається, оброблюється і передається в комп'ютерних системах і мережах», п. 2 «Організація, архітектура, методологія проектування, технологія функціонування СЗІ» і п. 3 «Математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем та криптографічних протоколів».

8. Зауваження щодо змісту дисертації:

1. У роботі не наведено часові показники формування кодових слів факторіальних кодів і не виконано їх порівняння з відповідними показниками інших кодів.
2. Незрозуміло, чому в виразі 2.12 (сторінка 118) під час оцінки кількості помилок, здатних перетворити одну дозволену комбінацію в іншу, кратність помилок обмежена автором до чотирьох.
3. Автором роботи виконано аналіз показників достовірності передавання інформації при застосуванні факторіального кодування даних для ймовірності помилки в каналі зв'язку 10^{-3}. Але канали зв'язку можуть відрізнятися за цим показником. Тому очевидним є питання щодо ефективності запропонованих принципів факторіального кодування для різних каналів зв'язку з різною фізичною природою.
4. Алгоритм, реалізований пристроєм формування послідовностей псевдовипадкових чисел на основі лінійного конгруентного генератора з будь-яким графом станів, структурна схема якого наведена на сторінці 241, має значну просторову складність за великих значень *M*. Доцільно було б оцінити цю складність та надати рекомендації щодо практичного застосування розробленого алгоритму.
5. Доцільно було б дослідити випадкову послідовність перестановок за допомогою діаграм Юнга (за В.І. Арнольдом).
6. Автор зосереджує увагу на дослідженні умов отримання лише рівномірного закону розподілу дискретної випадкової величини на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем. На мою думку, доцільно було б розглянути також і інші закони розподілу, зокрема, нормальний.

7. У роботі наведено деякі оцінки стійкості криптографічних перетворень на основі факторіального кодування даних до атаки прямого перебору ключів. Але не проведено оцінок стійкості щодо відомих методів криптоаналізу, зокрема, актуальних для найближчого майбутнього методів криптоаналізу з використанням квантових комп'ютерів.
8. Наведені в четвертому розділі елементи теорії графів, зокрема, графів-циклів, (сторінки 212-214) та основи теорії алгебри монад і топології їх графів (сторінки 214-216) доцільно було б перенести до першого розділу дисертації.

9. Висновок. Дисертаційна робота Фауре Еміля Віталійовича представляє собою завершену наукову роботу на актуальну тему, а одержані результати вирішують важливу науково-технічну проблему розробки методології захисту інформації на основі факторіального кодування даних з необхідними властивостями кодових послідовностей для побудови інтегрованих систем захисту інформації від несанкціонованого доступу та модифікації , а також природних завад у каналах зв'язку.

Дисертаційна робота відповідає вимогам «Порядку присудження наукових ступенів», а її автор – Фауре Еміль Віталійович – заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент:
директор Навчально-наукового
інституту «Радіо, телебачення та
інформаційної безпеки»
Одеської національної академії
зв`язку ім. О.С. Попова,
доктор технічних наук, професор Є.В. Василіу

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ ім. О.С. ПОПОВА Код в ЄДРПОУ 01

ПІДПИС ЗАВІРЯЮ:
УЧЕНИЙ СЕКРЕТАР
ОНАЗ ім. О.С. ПОПОВА
РУДА Г.В.