Голові спеціалізованої вченої ради Д 26.062.17
при Національному авіаційному університеті

ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА
професора кафедри безпеки інформаційних технологій
Національного авіаційного університету, доктора технічних наук, доцента
Казмірчук Світлани Володимирівни
на дисертаційну роботу
Фауре Еміля Віталійовича
«Методологія захисту інформації на основі факторіального кодування даних»,
представлену на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.21 – системи захисту інформації

1. Актуальність теми дисертації

Зі швидким розвитком та впровадженням інформаційних систем, телекомунікаційних мереж різноманітного призначення, розподілених баз даних тощо, з одночасним збільшенням кількості загроз інформаційної безпеки та досить легкого і всебічного доступу до інформації через мережу Інтернет зростає потреба у забезпечені захисту інформації. У цих умовах впроваджуються захищені операційні системи та інші програмні засоби, що забезпечують захист і розмежування доступу користувачів до інформації в окремих комп'ютерах та розподілених інформаційно-комунікаційних системах і мережах. Завдання забезпечення безпеки інформації залежать від можливих загроз, що можуть виникати в кожному окремому випадку та пов'язані із запобіганням несанкціонованого доступу, модифікації, підміни, спотворення, переадресування, недопустимої затримки передавання повідомлення та інших можливостей впливу на інформацію. Одночасна реалізація декількох видів захисту, по-перше, вимагає підвищеної продуктивності засобів обробки інформації, що може бути критичним для їх мікроелектронного виконання, а, по-друге, призводить до значної надлишковості даних для забезпечення заданих рівнів імітостійкості та достовірності. Таким чином, на сьогоднішній день існують протиріччя між необхідністю реалізації декількох видів захисту інформації та обмеженою продуктивністю технічних засобів її обробки, а також необхідністю введення надлишковості для забезпечення заданих показників захищеності інформації та обмеженою пропускною здатністю каналів зв'язку.

Виходячи з цього, створення, дослідження та розвиток підходів, принципів, методів і засобів забезпечення безпеки інформації, що реалізують її інтегрований захист від декількох загроз, мінімізуючи при цьому введену

надлишковість, дозволить підвищити ефективність обробки інформації під час передавання та зберігання в інформаційно-комунікаційних системах і мережах.

Таким чином, дисертаційна робота Фауре Е.В., яка направлена на вирішення проблеми розробки методології захисту інформації на основі факторіального кодування даних для побудови систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу, є актуальною.

2. Аналіз основного змісту, наукової новизни і практичної цінності, достовірності та обґрунтованості результатів.

Аналіз основного змісту, наукової новизни та практичної цінності

Дисертація складається зі вступу, шести розділів, висновків, додатків і списку використаних джерел, що містить 355 найменувань. Загальний обсяг дисертації складає 477 сторінок, у тому числі 312 сторінок основного тексту. Робота містить 104 таблиці та 80 рисунків.

Зміст роботи відповідає поставленим у ній задачам.

У вступі обґрунтовано актуальність теми дослідження, чітко сформульовано мету та задачі роботи, які дозволяють вирішити поставлену проблему, представлено наукову новизну та практичну цінність отриманих результатів, наведено відомості щодо їх апробації, публікацій та застосування.

У першому розділі автором виконано аналіз світового досвіду щодо існуючих підходів, методів і засобів, які реалізують сумісний захист інформації від помилок каналу зв'язку, несанкціонованого доступу та/або модифікації даних, а також методів формування й оцінювання псевдовипадкових послідовностей (ПВП). Визначено основні задачі дослідження.

У другому розділі отримано наступні наукові та практичні результати:

– *удосконалено* метод формування випадкової послідовності перестановок на основі використання факторіальної системи числення (ФСЧ), який за рахунок того, що символи додаткового генератора випадкових чисел (ГВЧ) підсумовуються з модифікованим синдромом попередньої перестановки та визначають синдром наступної перестановки, дозволяє зменшити обсяг внутрішньої пам'яті додаткового ГВЧ не менш ніж на кількість біт, що дорівнює логарифму двійковому від порядку генерованих перестановок, уникнути порушення рівномірності їх розподілу та підвищити швидкість їх формування;

– *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 під

час передавання в телекомунікаційних системах в умовах обмежень пропускної здатності каналів зв'язку;

– *вперше* розроблено математичну модель процесу декодування роздільних факторіальних кодів, яка за рахунок дослідження механізмів перетворення в симетричному двійковому каналі одного кодового слова в інше дозволяє оцінити показники достовірності передавання інформації в результаті застосування факторіального кодування та підтвердити його ефективність за цими показниками порівняно з іншими методами завадостійкого кодування;

– розроблено структурну схему та алгоритм роботи пристрою формування випадкової послідовності перестановок, що забезпечують можливість його практичної реалізації та дозволяють підвищити швидкість формування перестановок порівняно з алгоритмом Фішера-Йєтса;

– розроблено структурні схеми та алгоритми роботи пристроїв кодування та декодування роздільних факторіальних кодів, що надають можливість їх практичної реалізації та дозволяють досягти енергетичний виграш у порівнянні з використанням циклічного надлишкового коду за однакових обсягів введеної надлишковості.

У третьому розділі отримано наступні наукові та практичні результати:

– *вперше* 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 каналу зв'язку та несанкціонованого доступу, а також підвищити її достовірність під час передавання в телекомунікаційних системах в умовах обмежень пропускної здатності каналів зв'язку;

– розроблено структурні схеми та алгоритми роботи пристроїв кодування та декодування нероздільних факторіальних кодів, що надають можливість їх практичної реалізації та дозволяють досягти енергетичний виграш у порівнянні з використанням циклічного надлишкового коду за однакових обсягів введеної надлишковості.

У четвертому розділі отримано наступні наукові та практичні результати:

– *удосконалено* метод формування ПВП на основі лінійного конгруентного методу, який за рахунок розробленої моделі узагальненого графа станів лінійного конгруентного генератора (ЛКГ) та представлення кожної зв'язної компоненти графа у вигляді циклів, оснащених добутками дерев, шляхом конкатенації в графі станів ЛКГ не лише відособлених непересічних циклів, а і передциклів (дерев), якщо вони в ньому містяться, дозволяє формувати ПВП рівномірно розподілених чисел максимального періоду незалежно від топології

графа станів ЛКГ, мінімізувати 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;

– *удосконалено* метод симетричного 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 виключити можливість винесення гами, зменшити ймовірність зламу шифру методом повного перебору ключового простору та підвищити стійкість до статистичного криптоаналізу;

– розроблено структурну схему та алгоритм роботи пристрою формування ПВП перестановок на основі ЛКГ з будь-яким типом графа його станів, що забезпечують можливість його практичної реалізації та дозволяють підвищити швидкість формування перестановок порівняно з алгоритмом Фішера-Йєтса;

– розроблено структурну схему та алгоритм роботи пристрою двоконтурного криптографічного перетворення даних, що забезпечують можливість його практичної реалізації та дозволяють виключити можливість винесення гами, забезпечити скінченний трек помилки та зменшити в порівнянні з використанням тільки першого контуру ймовірність зламу шифру методом повного перебору ключового простору.

У п'ятому розділі отримано наступні наукові та практичні результати:

– *вперше* 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, за рахунок визначення закону розподілу д.в.в. на виході такого 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 ФСЧ;

– розроблено методику вибору параметрів первинних генераторів перестановок для комбінаційного генератора з комбінаційною функцією підсумовування за модулем, що дозволяє забезпечити рівномірний розподіл сформованої д.в.в. на множині цілих чисел потужності M та проходження пакетів статистичного тестування ПВП NIST STS, Diehard, TestU01.

У шостому розділі отримано наступні наукові та практичні результати:

– *вперше* 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, притаманні послідовностям, породженим природними джерелами дискретного білого шуму, і не притаманні штучно згенерованим ПВП;

– *вперше* розроблено 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 забезпечити підтримку процесів створення систем інтегрованого захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу;

– розроблено критерії та методики перевірки послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, що можуть бути використані під час оцінювання випадкових послідовностей, у тому числі сумісно з пакетами статистичного тестування.

До основних результатів *наукової новизни*, які отримані в дисертаційній роботі, можна віднести:

– *удосконалений* метод формування випадкової послідовності перестановок на основі використання ФСЧ для зменшення обсягу внутрішньої пам'яті додаткового ГВЧ, уникнення порушення рівномірності їх розподілу та підвищення швидкості їх формування;

– *вперше* розроблені методи роздільного факторіального кодування інформації для забезпечення контролю цілісності інформації та підвищення її достовірності;

– *вперше* розроблені методи нероздільного факторіального кодування інформації для забезпечення захисту інформації від помилок каналу зв'язку та несанкціонованого доступу, а також підвищення її достовірності;

– *вперше* розроблену математичну модель процесу декодування факторіальних кодів для оцінювання показників достовірності передавання інформації в результаті застосування факторіального кодування;

– *удосконалений* метод формування ПВП на основі лінійного конгруентного методу для формування ПВП рівномірно розподілених чисел максимального періоду незалежно від топології графа станів ЛКГ, мінімізації часових витрат на вибір параметрів ЛКГ та збільшення розміру простору їх допустимих значень для досягнення максимального періоду;

– *удосконалений* метод симетричного криптографічного захисту інформації на основі операції гамування для виключення можливості винесення гами,

зменшення ймовірності зламу шифру методом повного перебору ключового простору та підвищення стійкості до статистичного криптоаналізу;

– *вперше* теоретично обґрунтовані принципи побудови комбінаційного генератора з комбінаційною функцією підсумовування за модулем для забезпечення необхідних статистичних властивостей ПВП;

– *вперше* розроблений метод оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел для їх тестування;

– *вперше* розроблену методологію захисту інформації на основі факторіального кодування даних для підтримки процесів створення систем інтегрованого захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу.

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

Отримані автором роботи наукові результати є логічними та чітко обґрунтованими на основі використання класичних і сучасних положень теорії захисту інформації, теорії завадостійкого кодування, теорії факторіального числення, математичного моделювання, теорії ймовірностей і математичної статистики, кореляційного аналізу.

Наукові результати роботи в достатній мірі апробовано на міжнародних і всеукраїнських наукових конференціях.

Додатково достовірність отриманих результатів підтверджено їх використанням у виробничому та навчальному процесах, що відображено у відповідних актах впровадження.

Оцінка мови та стилю викладання дисертації та автореферату

Дисертація та автореферат написано та оформлено грамотно, а стиль викладення в них наукових положень, висновків і рекомендацій відповідає вимогам до звітів у сфері науки і техніки.

Зміст автореферату повністю відображає основні положення дисертації.

Повнота викладення наукових результатів дисертації в опублікованих працях

Основний зміст, наукові положення та результати дисертаційного дослідження викладено в 80 наукових працях, основні 60 з яких наведено в авторефераті. Серед них: 2 розділи в 2 колективних монографіях, 4 наукові статі у виданнях, що входять до наукометричних баз даних Scopus / Web of Science, 2 наукові статті у закордонних фахових наукових журналах та 27 наукових статей у вітчизняних фахових наукових журналах, які входять до інших міжнародних наукометричних баз даних, а також 13 матеріалів і тез доповідей наукових конференцій.

Зазначені публікації в повній мірі висвітлюють основні наукові результати дисертації.

Зауваження та недоліки до тексту дисертації та автореферату:

1) у роботі не наведено перелік конкретних прикладних задач, для яких актуальна розв'язувана в роботі проблема. Доцільно було б показати, в яких саме застосуваннях з'являються вказані в роботі протиріччя між необхідністю реалізації декількох видів захисту інформації та обмеженою продуктивністю технічних засобів її обробки, а також необхідністю введення надлишковості для забезпечення заданих показників захищеності інформації та обмеженою пропускною здатністю каналів зв'язку;

2) з метою перевірки точності оцінки кількості помилок, здатних перетворити перестановку в перестановку, (наприклад, визначеної виразом (2.12) (сторінка 118)) доцільно було б навести відповідні результати експериментального розрахунку подібно результатам, отриманим P. Koopman для CRC-коду;

3) під час визначення ймовірності не виявленої декодером факторіального коду помилки автор робить припущення про незалежність бітових помилок у каналі зв'язку (наприклад, на сторінці 117), хоча в реальних умовах помилки дуже часто групуються;

4) викликає сумніви правомірність оцінки ймовірності зламу ПФК у вигляді, представленому на сторінці 114, оскільки вона отримана виходячи передумови, що в якості перевірної частини кодового слова допустиме використання будь-якого поєднання заданої кількості символів перестановки. Це може бути і не так, оскільки достовірність передавання може бути різною для різних наборів цих символів. Ступінь відмінності достовірності передавання для різних наборів також не визначено;

5) викликає сумніви правомірність використання у множині дозволених таблиць замін усіх сполучень з 2^k перестановок із $M!$ можливих у виразі для ймовірності зламу нероздільного факторіального коду з декількома контрольними сумами (сторінка 180), оскільки під час виведення цього виразу передбачається, що достовірність передавання не залежить від складу перестановок і їх розташування в таблиці. Це припущення не підтверджене;

6) автором не визначено критерії оптимальності вибору класу перестановок для методу факторіального кодування з заданим числом інверсій;

7) у роботі недостатньо висвітлено чисельні показники захищеності інформації внаслідок застосування розробленого автором двоконтурного криптографічного перетворення інформації;

8) автором у різних розділах роботи однаковими символами позначено різні змінні (наприклад, у розділах 2, 3 символом M позначається порядок перестановки, у розділах 4, 5 – модуль, за яким обчислюється значення генератора псевдовипадкових чисел).

Зазначені недоліки не є визначальними. Вони не впливають на загальне позитивне враження від роботи, не зменшують її наукової цінності та практичної значущості.

3. Загальний висновок по роботі.

Дисертація Фауре Еміля Віталійовича «Методологія захисту інформації на основі факторіального кодування даних» є завершеною кваліфікаційною працею та свідчить про особистий внесок автора в науку.

За своєю актуальністю, рівнем наукової новизни та практичною значущістю отриманих результатів дисертаційна робота Фауре Е.В. відповідає паспорту спеціальності 05.13.21 – Системи захисту інформації, а також вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, а її автор – Фауре Еміль Віталійович – заслуговує на присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – Системи захисту інформації.

Офіційний опонент:
професор кафедри
безпеки інформаційних технологій
Національного авіаційного університету,
доктор технічних наук, доцент С.В. Казмірчук

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
01680 м. Київ
МІСТО КИЇВ

С.В. Казмірчук
З а с в і д ч у ю
Вчений секретар
Національного авіаційного університету
Г. Сичева