ВІДГУК

офіційного опонента на дисертаційну роботу

Харіна Олександра Олександровича

«Методи та засоби інтегрованого захисту інформації в телекомунікаційних системах множинного доступу на основі факторіального кодування даних»,

представлену на здобуття ступеня

доктора філософії

за спеціальністю 123 – Комп'ютерна інженерія

1. Актуальність теми дисертаційної роботи.

Комп'ютеризація виробничої та економічної діяльності стимулює повсюдне застосування складних керуючих систем, в тому числі систем дистанційного укладання угод і розрахунків за ними. Як наслідок, посилюється загальний інтерес до забезпечення захисту інформації як від помилок, спричинених дією завад у каналах зв'язку, так і від несанкціонованого читання інформації, що циркулює в тракті «виробництво товару – продаж товару – розрахунок за товар». Крім того, важливою задачею є забезпечення цілісності інформації. Тому актуальним напрямом досліджень на сьогоднішній день є забезпечення інтегрованого захисту інформації від декількох чинників – несанкціонованого доступу та несанкціонованої модифікації, а також помилок у каналі зв'язку. Одним з підходів, спрямованих на забезпечення такого інтегрованого захисту, базується на використанні методів факторіального кодування інформації, що передбачає використання перестановок як носія інформації.

На сьогоднішній день перспективним є дослідження можливості використання факторіальних кодів у спеціалізованих комп'ютерних і телекомунікаційних системах, де є необхідність забезпечення заданого рівня достовірності передавання даних, у тому числі мовленнєвих, в умовах погіршення якості каналу зв'язку в результаті впливу природних та техногенних чинників.

Таким чином, дисертаційна робота Харіна Олександра Олександровича «Методи та засоби інтегрованого захисту інформації в телекомунікаційних системах множинного доступу на основі факторіального кодування даних» є актуальною на сучасному етапі розвитку науки і техніки.

2. Наукова новизна результатів роботи.

У дисертаційній роботі вирішується науково-технічна задача, що полягає в підвищенні достовірності передавання інформації, забезпеченні її конфіденційності та цілісності на основі використання факторіального кодування даних. Ця задача передбачає необхідність удосконалення існуючих методів факторіального кодування, а також створення методу побудови телекомунікаційних систем на основі нероздільного факторіального кодування з динамічним розподілом ресурсів між користувачами системи в режимі

реального часу. Автором отримано наступні наукові результати:

- вперше розроблено методи підвищення достовірності передавання даних у системах з факторіальним кодування з відновленням даних за перестановкою, які за рахунок доповнення перестановки бітами ознак та комбінування завадостійких кодів дозволяють підвищити здатність нероздільних факторіальних кодів до виявлення помилок;
- вперше розроблено метод формування сигнально-кодової конструкції для систем з факторіальним кодування з відновленням даних за перестановкою, який за рахунок побудови решіток з високою щільністю розташування сигнальних векторів дозволяє максимізувати швидкість коду для заданого рівня достовірності передавання даних та відповідної мінімальної відстані між вузлами решітки;
- отримав подальший розвиток метод факторіального кодування з відновленням даних за перестановкою, який за рахунок відновлення даних з втратами на основі метрики Хеммінга або методу лінійної інтерполяції дозволяє забезпечити захист мовленнєвої інформації від помилок каналу зв’язку та несанкціонованого доступу в телекомунікаційних системах реального часу;
- вперше розроблено метод побудови систем множинного доступу на основі нероздільного факторіального кодування, який за рахунок використання факторіального коду з заданим числом інверсій та виділення кожному з користувачів підмножини перестановок з певним набором властивостей забезпечує інтегрований захист інформації від несанкціонованого доступу та помилок каналу зв'язку, а також циклову синхронізацію без застосування окремого каналу синхронізації.

Практичне значення отриманих результатів полягає в наступному:

- розроблено алгоритм факторіального кодування з додатковими перевірними бітами. Реалізація алгоритму дає змогу зменшити ймовірність невиявленої кодом помилки, за незалежних бітових помилок, у порівнянні з факторіальним кодом з відновленням даних за перестановкою з доповненням (ФКВДд) на 2-4 порядки для $M = 8$ у залежності від імовірності бітової помилки за рахунок незначної втрати в швидкості коду;
- розроблено алгоритм факторіального каскадного кодування. Реалізація алгоритму дає змогу на порядок зменшити ймовірність невиявленої кодом помилки, за незалежних бітових помилок, у порівнянні з ФКВД для $k = 15$ у залежності від ймовірності бітової помилки, при цьому за довжини блоку даних $k \geq 128$ швидкість коду не змінюється;
- побудовано решітки, вузлами якої є перестановки, що дозволяють виявляти помилки кратності $t \leq 5$ і виправляти помилки кратності $t \leq 2$ з максимальною швидкістю коду для $M = 5,\ k = 3,\ N_{sv} = 10$ та $M = 6,\ k = 5,\ N_{sv} = 60$;

- розроблено структурну схему пристрою декодування та алгоритм виправлення помилок з втратами у нероздільних факторіальних кодах в метриці Хеммінга, що забезпечує рівень шуму декодування, який не перевищує значень рівня комфортного шуму за ймовірності бітової помилки $p_0 \leq 10^{-2}$ у каналах з незалежними бітовими помилками. Розроблена схема дозволяє апаратно реалізувати пристрій декодування факторіальних кодів в метриці Хеммінга.

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

Виконані в роботі дослідження базуються на коректному використанні положень:

- дискретної математики;
- теорії ймовірності і математичної статистики;
- цифрової обробки інформації;
- теорії інформації;
- статистичного аналізу;
- комп'ютерних мереж;
- об'єктно-орієнтованого програмування.

4. Повнота викладу в наукових публікаціях, зарахованих за темою дисертації.

Результати дослідження опубліковано в 18 наукових працях, у тому числі в трьох наукових статтях, що входять до наукометричних баз даних Scopus та/або Web of Science, двох статтях у наукових виданнях, що входять до переліку фахових видань МОН України та інших наукометричних баз даних, семи доповідях на науково-практичних конференціях і шести патентах України на корисні моделі. Кількість та якість публікацій, опублікованих за матеріалами дисертаційного дослідження, відповідають встановленим вимогам МОН України.

5. Ідентичність змісту анотації основним положенням дисертації.

Аналіз дисертації Харіна О.О. на предмет ідентичності змісту опублікованої анотації засвідчує відповідність її основним положенням. Анотацію та текст дисертації оформлено відповідно до вимог МОН України.

6. Зауваження щодо змісту дисертаційної роботи.

У роботі присутні деякі недоліки, а саме:

1) у першому розділі дисертаційної роботи (сторінки 40-41) розглядається лише базовий алгоритм кодування-декодування згорткових кодів, у той час, коли існують більш сучасні методи декодування;

2) у другому розділі дисертаційної роботи (сторінка 53) запропоновано метод факторіального кодування з додатковими перевірними бітами, що передбачає різні алгоритми формування перевірних біт, однак оцінку показників достовірності передавання даних виконано лише для одного з наведених алгоритмів;
3) для методу факторіального каскадного кодування як внутрішній код використовується рівноважний код (сторінка 60), проте такий вибір не є оптимальним з точки зору наділення коду новими властивостями, оскільки факторіальний код також є рівноважним;
4) розроблені в другому розділі методи факторіального кодування порівнюються з іншими факторіальними кодами, в той час як доцільно було б також виконати порівняння з іншими відомими методами завадостійкого кодування, наприклад, CRC-кодами;
5) у роботі, зокрема, в другому розділі, не проведено оцінювання стійкості до зламу розроблених методів факторіального кодування, хоча автором наголошувалось на забезпеченні інтегрованого захисту інформації;
6) у третьому розділі для методу формування сигнально-кодової конструкції виконано побудову решіток потужністю 10 та 60 вузлів, що обмежує область використання таких конструкцій в зв’язку з малою потужністю множини кодових слів;
7) у четвертому розділі доцільно було б виконати порівняння розроблених методів декодування мовленнєвої інформації з іншими відомими методами;
8) у вихідному коді розрахунково-експериментальних моделей, запропонованих у роботі (додаток А), для деяких методів відсутні пояснюючі коментарі, що ускладнює його розуміння.

Наведені зауваження не мають принципового характеру і не впливають на загальну позитивну оцінку дисертаційної роботи.

7. Дотримання принципів академічної доброчесності.

Результати аналізу роботи, в тому числі за допомогою перевірки тексту дисертації з використанням Системи виявлення текстових збігів, свідчать про відповідність дисертації принципам академічної доброчесності.

8. Висновок.

Дисертація Харіна Олександра Олександровича «Методи та засоби інтегрованого захисту інформації в телекомунікаційних системах множинного доступу на основі факторіального кодування даних» є завершеною науково-дослідницькою працею. Результати, отримані автором, можуть бути використані в системах передавання даних, що потребують реалізації інтегрованого захисту в єдиній процедурі.

Дисертаційна робота за своїм змістом відповідає освітньо-науковій

програмі «Комп'ютерні системи та мережі» за спеціальністю 123 – Комп'ютерна інженерія.

За актуальністю обраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю й обґрунтованістю висновків, новизною та значенням отриманих результатів для науки і практичного використання дисертаційна робота задовольняє вимогам «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)» і «Порядку проведення експерименту з присудження ступеня доктора філософії», а її автор, Харін Олександр Олександрович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія.

Офіційний опонент:
завідувач кафедри
обчислювальної техніки та програмування
Національного технічного університету
«Харківський політехнічний інститут»,
доктор технічних наук, професор Сергій Семенов

Підпис
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
Заковоротний О.Ю.
"08" 09 2020 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * код 02071180 *