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», подану на здобуття ступеня
доктора філософії
за спеціальністю 123 Комп'ютерна інженерія

1. Актуальність обраної теми дисертації.

Важко переоцінити важливість криптографічних методів та засобів захисту інформації для сучасних комп'ютерних та телекомунікаційних мереж. Криптографічні додатки повсякденно використовуються для захисту персональних даних, передавання інформації з обмеженим доступом відкритими каналами зв'язку. Це особливо проявляється в фінансовій та комерційній діяльності, сфері дистанційного керування автоматизованими виробничими комплексами і процесами, а також в сферах діяльності силових і охоронних відомств. З іншого боку, чітко простежується тенденція до розширення функціональних можливостей портативних пристроїв, що характеризуються обмеженим об'ємом ресурсів. Зважаючи на це, розробка методів кодування інформації, які дозволяють реалізувати функції завадостійкого кодування та криптографічного захисту інформації в єдиній процедурі та на єдиній апаратній платформі, є перспективним напрямком дослідження.

Одним з існуючих на сьогодні підходів до поєднання завадостійкого кодування та криптографічного захисту є використання перестановок та факторіальної системи числення. Цей підхід реалізує компроміс між достовірністю передавання даних, з одного боку, та відносною швидкістю передавання й швидкістю коду, з іншого.

Проте потребує подальшого розгляду питання використання факторіальних кодів в системах, де існує потреба в забезпеченні заданого рівня QoS в умовах погіршення якості каналу зв'язку. Крім того, актуальною є задача розробки методів факторіального кодування, орієнтованих на кодування мовленнєвої інформації в системах реального часу.

Враховуючи наведені аргументи, актуальність теми дисертаційного дослідження Харіна Олександра Олександровича «Методи та засоби

інтегрованого захисту інформації в телекомунікаційних системах множинного доступу на основі факторіального кодування даних» не викликає жодних сумнівів.

2. Ступінь обґрунтованості наукових положень дисертації та їх достовірність.

Основні наукові результати дослідження: методи підвищення достовірності передавання нероздільних факторіальних кодів, методи факторіального кодування мовленнєвих сигналів та метод побудови систем множинного доступу на основі факторіальних кодів – чітко сформульовані, достатньо обґрунтовані та не викликають сумнівів. Достовірність наукових положень дисертації забезпечується:

– коректним використанням у процесі досліджень методів теорії ймовірності і математичної статистики, методів кодування інформації, комп'ютерної криптографії, статистичного аналізу, теорії інформації та комбінаторики;

– відповідністю проведених експериментальних досліджень за допомогою розроблених програмних моделей виконаним теоретичним розрахункам.

3. Наукова новизна отриманих результатів полягає в наступному:

– 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.

4. Практична цінність результатів полягає у 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 ймовірності 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.

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

Основні наукові результати, що отримані в дисертації, викладено здобувачем у 18 друкованих працях, в тому числі в 3 наукових статтях, що входять до наукометричних баз даних Scopus та/або Web of Science, 2 статтях у наукових виданнях, що входять до переліку МОН України та інших наукометричних баз даних, та 7 доповідях на науково-практичних конференціях. Отримано 6 патентів України на корисні моделі.

6. Дотримання норм академічної доброчесності

Аналіз дисертації Харіна О.О. свідчить про дотримання автором норм і правил академічної доброчесності. Некоректно оформлених запозичень чи інших ознак неправомірного використання результатів інших авторів без зазначення авторства в роботі не виявлено.

7. Зауваження по дисертації:

– у оглядовій частині дисертації автором розглянуто тільки деякі методи організації множинного доступу. Зокрема, не досліджено та, відповідно, не порівняно властивості запропонованої системи з множинним доступом на основі факторіального кодування з системами множинного доступу з кодовим та частотним розділенням каналів;

– автором роботи не досліджено ефективність атак на розроблені факторіальні коди та не виконано оцінку їх криптографічної стійкості;

– у другому розділі для методу факторіального кодування з додатковими перевірними бітами описано алгоритм роботи кодека та проведено оцінку завадостійкості лише для одного перевірного біта. Доцільно було б також розглянути та оцінити ефективність застосування більшої кількості додаткових біт, а також комбінації різних алгоритмів їх формування;

– у дисертаційній роботі, зокрема в третьому та четвертому розділах, для оцінки показників достовірності передавання даних розроблено програмні моделі, проте не в достатній мірі описано алгоритм їхньої роботи, що ускладнює розуміння процесу моделювання;

– автором не оцінено часову та просторову складності алгоритму формування сигнально-кодової конструкції для систем з факторіальним кодуванням з відновленням даних за перестановкою для досягнення максимальної швидкості коду для заданого рівня достовірності передавання даних та відповідної мінімальної відстані між вузлами решітки;

– не виконано розрахунок часу, який витрачається на встановлення синхронізму за робочим сигналом для канального мультиплексора на основі факторіальних кодів;

– не виконано порівняння якісних показників побудованої системи з множинним доступом з іншими наведеними в дисертаційній роботі аналогами;

– для розробленої системи з множинним доступом на основі факторіального кодування даних автором не досліджено залежність швидкості коду від кількості користувачів системи та довжини перестановки. Результати такого дослідження були б корисними для порівняльної оцінки з іншими

системами та для вибору оптимальних показників розробленої системи.

Наведені недоліки не зменшують значимість отриманих наукових результатів.

8. Висновок. Дисертаційна робота Харіна Олександра Олександровича представляє собою завершену наукову роботу на актуальну тему, а отримані результати вирішують важливу науково-технічну задачу підвищення достовірності передавання інформації, забезпечення її конфіденційності та цілісності на основі використання факторіального кодування даних.

Представлена до розгляду дисертація відповідає вимогам МОН України, зокрема 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 кібербезпеки та
програмного забезпечення
Центральноукраїнського національного
технічного університету,
доктор технічних наук, професор О.А. Смірнов

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи
Центральноукраїнського національного
технічного університету,
доктор економічних наук, професор О.М. Левченко
"18" 09 2020 року