МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ФАУРЕ Еміль Віталійович

УДК 004.056.53:004.056.2:004.421.5(043.3)

МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ФАКТОРІАЛЬНОГО КОДУВАННЯ ДАНИХ

05.13.21 – системи захисту інформації

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2018

Дисертацією є рукопис.

Робота виконана в Черкаському державному технологічному університеті Міністерства освіти і науки України.

Науковий консультант: доктор технічних наук, професор
Рудницький Володимир Миколайович,
Черкаський державний технологічний університет, проректор з науково-дослідної роботи та міжнародних зв'язків.

Офіційні опоненти: доктор технічних наук, професор
Халімов Геннадій Зайдулович,
Харківський національний університет радіоелектроніки, завідувач кафедри безпеки інформаційних технологій;

доктор технічних наук, професор
Василіу Євген Вікторович,
Одеська національна академія зв`язку ім. О.С. Попова, директор Навчально-наукового інституту «Радіо, телебачення та інформаційної безпеки»;

доктор технічних наук, доцент
Казмірчук Світлана Володимирівна,
Національний авіаційний університет, професор кафедри безпеки інформаційних технологій.

Захист відбудеться «27» вересня 2018 р. о 14^{00} год. на засіданні спеціалізованої вченої ради Д 26.062.17 Національного авіаційного університету за адресою: 03058, Київ, пр. Космонавта Комарова, 1, корпус 11, ауд. 111.

З дисертацією можна ознайомитися в науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «27» серпня 2018 р.

Учений секретар
спеціалізованої вченої ради С.О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність тими дослідження. Інтенсивна комп'ютеризація всіх видів виробничої, управлінської та інформаційної діяльності призводить до повсюдного впровадження телекомунікаційних систем і мереж. Їх використання в сферах оборони, комерційної діяльності, дистанційного керування фінансовими операціями й електронного документообігу вимагає передавання конфіденційної інформації та забезпечення її цілісності, що досягається засобами криптографічного захисту.

Через безперервне зростання об'ємів передавання інформації, в тому числі конфіденційної, а також сформоване конкурентне середовище процесів створення й удосконалення систем атаки та систем захисту зростає математико-логічна складність і ступінь інтелектуалізації використовуваних алгоритмів, процесів і технічних засобів. Це призводить до необхідності підвищення ефективності та гарантоздатності (надійності та безпеки) телекомунікаційних систем і мереж, а також їх компонентів, що реалізовують функції захисту інформації.

Під час передавання інформації в системах зв'язку й управління різноманітного призначення, у тому числі на основі тунельованих протоколів комп'ютерних мереж, одночасно вирішуються декілька задач захисту інформації – забезпечення аутентифікації, конфіденційності, цілісності. Окреме вирішення цих задач пов'язане з застосуванням різних математичних методів і алгоритмів, а також послідовною обробкою інформації, що призводить до збільшення навантаження на засоби перетворення інформації та підвищення вимог до їх швидкодії, збільшення введеної надлишковості і, як наслідок, до зменшення відносної швидкості передавання. Ці обставини актуалізують проблему забезпечення захисту інформації під час її зберігання та передавання в телекомунікаційних системах і мережах за рахунок інтеграції методів канального кодування та криптографічного захисту, що реалізують сумісний захист переданих даних від помилок каналу зв'язку, а також несанкціонованої модифікації та/або несанкціонованого доступу. Актуальність зазначеної проблеми підтверджується також тим, що за даними NIST одними з найбільш перспективних напрямів постквантової криптографії є криптографія на основі кодів виправлення помилок та на основі решіток.

Забезпечення інтегрованого захисту інформації від помилок каналу зв'язку, а також несанкціонованої модифікації та/або несанкціонованого доступу передбачає розв'язання супутніх задач, пов'язаних з удосконаленням існуючих і розробкою нових методів формування й оцінювання послідовностей випадкових і псевдовипадкових (ПВП) чисел. Зауважимо, що якість цих послідовностей має вирішальне значення в питаннях забезпечення безпеки зберігання, транспортування й обробки даних, у тому числі тих, що розглядаються в цій роботі.

Фундаментальні основи теорій криптографічного захисту інформації та її завадостійкого кодування розробив C.E. Shannon. Значний вклад у їх розвиток внесли дослідники: H. Feistel, W. Diffie, M. E. Hellman, R. L. Rivest, A. Shamir, L. Adleman, R. Hamming, W. W. Peterson, A. Hocquenghem, R. Bose, D. K. Ray-Chaudhuri, R. J. McEliece, С. А. Осмоловський, О. П. Стахов, М. І. Мазурков,

В. Я. Чечельницький, О. А. Борисенко, В. А. Лужецький, В. М. Рудницький. Задачам формування послідовностей випадкових і псевдовипадкових чисел, а також їх оцінки присвячено роботи D. H. Lehmer, R. C. Tausworthe, R.R. Coveyou, G. Marsaglia, D.E. Knuth, P. L'Ecuyer, H. Niederreiter, S. K. Park, K. W. Miller, M. Matsumoto, T. Nishimura, M. J. B. Robshaw, І. Д. Горбенка, М. О. Іванова, І. В. Чугункова та ін.

Відомі підходи до поєднання завадостійкого кодування та криптографічного захисту на сьогоднішній день базуються на: криптосистемі McEliece, універсальному стохастичному кодуванні, «золотій» криптографії, досконалих алгебраїчних конструкціях, використанні перестановок. Перші три підходи мають складнощі в їх практичній реалізації. Підхід на основі досконалих алгебраїчних конструкцій є одним з найбільш розвинутих, проте призначений для широкосмугових систем зв'язку та не дозволяє контролювати цілісність даних. Використання ж перестановок і, відповідно, позиційної системи числення з факторіальною основою (факторіальної системи числення – ФСЧ) є перспективним, проте найменш розвинутим підходом.

Таким чином, на сучасному етапі розвитку науки та техніки існує *об'єктивне протиріччя* між потребою в реалізації декількох видів захисту інформації та максимізації достовірності передавання даних, з одного боку, та обмеженою смугою пропускання каналів зв'язку, необхідністю максимізації відносної швидкості передавання й швидкості коду та мінімізації введеної надлишковості, з іншого.

Вирішення цього протиріччя вважається можливим на основі розроблення теоретичних і методологічних засад інтеграції канального кодування та криптографічного захисту на основі перестановок і ФСЧ. Оскільки такий інтегрований захист передбачає введення надлишковості, що за своїми фізичними принципами відноситься до завадостійкого кодування, процес перетворення інформації для її захисту на основі ФСЧ будемо називати факторіальним кодуванням. Відповідно, отриманий у результаті факторіального кодування код будемо називати факторіальним кодом.

Враховуючи викладене, *актуальною науково-технічною проблемою* є розробка методології захисту інформації на основі факторіального кодування даних з необхідними ансамблевими, статистичними, структурними властивостями кодових послідовностей для побудови систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу із забезпеченням підвищення достовірності передавання інформації за однакових обсягів введеної надлишковості.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження, результати яких представлені в дисертаційній роботі, відповідають пріоритетному напряму розвитку науки і техніки України «Інформаційні та комунікаційні технології» та його тематичному напряму «Технології та засоби захисту інформації» і виконувалися відповідно до програм і планів науково-дослідних робіт Черкаського державного технологічного університету, у тому числі в рамках науково-дослідної теми «Синтез операцій криптографічного перетворення із заданими

характеристиками» (номер державної реєстрації 0116U008714), держбюджетної науково-дослідної теми «Розробка мобільного високоефективного ультразвукового хірургічного інструменту для військової та цивільної медицини» (номер державної реєстрації 0117U007474), в яких автор брав участь як виконавець.

Мета і задачі дослідження. Метою роботи є розробка методології захисту інформації на основі факторіального кодування даних для побудови систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу.

Аналіз існуючого стану науково-технічних, методологічних і практичних положень поєднання операцій захисту інформації від несанкціонованого доступу, захисту від нав'язування хибних даних і завадостійкого кодування, а також формування ПВП і оцінювання їх якості породжують наступні проблемні задачі:

− удосконалення методу формування випадкової послідовності перестановок та створення теоретичного базису для методів факторіального кодування даних;

− розробка методів роздільного факторіального кодування інформації для забезпечення її захисту від нав'язування хибних даних і помилок каналу зв'язку;

− розробка методів нероздільного факторіального кодування інформації для забезпечення її захисту від несанкціонованого доступу і помилок каналу зв'язку;

− розробка математичної моделі процесу декодування факторіальних кодів з метою оцінки ймовірності не виявленої декодером помилки;

− удосконалення методу формування ПВП на основі конкатенації зв'язних компонентів графа станів лінійного конгруентного генератора (ЛКГ) для створення елементів перетворення інформації в процесі факторіального кодування;

− удосконалення методу симетричного криптографічного захисту інформації для забезпечення її конфіденційності;

− теоретичне обґрунтування принципів побудови комбінаційного генератора, що використовує підсумовування за модулем у якості комбінаційної функції, для забезпечення необхідних статистичних властивостей під час вирішення задач захисту інформації; аналіз якості ПВП залежно від параметрів комбінаційного генератора і властивостей початкових послідовностей;

− розробка методу і критеріїв кореляційного аналізу часових рядів для тестування ПВП з метою оцінювання їх статистичних відхилень від теоретичних розподілів показників випадкового процесу;

− розробка методології захисту інформації на основі факторіального кодування даних.

Об'єктом дослідження є процеси захисту інформації в телекомунікаційних системах і мережах в умовах обмеженості пропускної здатності каналів зв'язку.

Предметом дослідження є моделі, методи та засоби забезпечення захисту інформації на основі факторіального кодування даних.

Методи досліджень, які використовуються в роботі, ґрунтуються на теорії факторіального числення для розробки методу формування випадкової послідовності перестановок; теорії криптографічного захисту інформації, теорії завадостійкого кодування для розробки методів факторіального кодування; теорії

ймовірностей для оцінки показників достовірності передавання інформації в результаті застосування факторіальних кодів; теорії алгебри монад і топології їх графів для дослідження топології графа станів ЛКГ, розвитку методу формування ПВП на основі ЛКГ та удосконалення методу двоконтурного криптографічного перетворення даних; теорії ймовірностей і статистичного аналізу для доведення тверджень щодо рівномірності розподілу дискретної випадкової величини (д.в.в.) комбінаційного генератора з комбінаційною функцією підсумовування за модулем; теорії статистичного аналізу коефіцієнтів автокореляції і їх знаків для розробки методу оцінювання послідовностей рівномірно розподілених випадкових чисел.

Наукова новизна отриманих результатів:

– *удосконалено* метод формування випадкової послідовності перестановок на основі використання ФСЧ, який за рахунок введення додаткового генератора випадкових чисел (ГВЧ), символи якого 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 (метод повного факторіального кодування, метод комбінованого факторіального кодування, метод факторіального кодування з проріджуванням, метод роздільного факторіального кодування з декількома контрольними сумами), 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* методи нероздільного факторіального кодування інформації (метод факторіального кодування з відновленням даних за перестановкою, метод факторіального кодування з відновленням даних за перестановкою з доповненням, метод нероздільного факторіального кодування з декількома контрольними сумами, метод факторіального кодування з відновленням даних за перестановкою з заданим числом інверсій, метод факторіального кодування з відновленням даних за перестановкою та виправленням помилок), 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;

– *вперше 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;

– *удосконалено* метод формування ПВП на основі лінійного конгруентного методу, який за рахунок розробленої моделі узагальненого графа станів 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;

– *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;

– *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.

Практичне значення отриманих результатів:

− розроблено структурну схему та алгоритм роботи пристрою формування випадкової послідовності перестановок порядку M, що забезпечують можливість його практичної реалізації та дозволяють уникнути приведення випадкових чисел до діапазону зі змінною верхньою межею, зменшити розрядність внутрішнього стану додаткового ГВЧ не менш ніж на $\log_2 M$ біт, а також підвищити швидкість формування перестановок порівняно з алгоритмом Фішера-Йєтса (зокрема, для додаткового генератора псевдовипадкових чисел (ГПВЧ) LFIB78 і $M = 5$ – у 2,1 рази; $M = 10$ – у 2,6 рази; $M = 20$ – у 2,8 рази);

− розроблено структурні схеми та алгоритми роботи пристроїв кодування та декодування факторіальних кодів (повного факторіального коду (ПФК), комбінованого факторіального коду (КФК), роздільного та нероздільного факторіальних кодів з декількома контрольними сумами (ФКДКСр і ФКДКСн відповідно), факторіального коду з відновленням даних за перестановкою (ФКВД), факторіального коду з заданим числом інверсій (ФКЗЧІ), факторіального коду з виявленням і виправленням помилок (ФКВДвп)), що надають можливість їх практичної реалізації, дозволяють забезпечити захист інформації та досягти енергетичного виграшу в порівнянні з використанням циклічного надлишкового коду за однакових обсягів введеної надлишковості, зокрема, для ймовірності помилки в каналі $p_0 = 10^{-3}$ та роздільного факторіального кодування: ПФК – до 2,7 дБ для довжини інформаційної частини $k = 1024$ біти та довжини перевірної частини $r = 64$ біти, КФК – до 1,6 дБ для $k = 1024$ біти та $r = 16$ біт; нероздільного факторіального кодування: ФКВД – до 0,821 дБ, ФКЗЧІ – до 3,295 дБ (для порядку перестановки 8);

− 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 мінімізувати часові витрати на вибір параметрів ЛКГ і збільшити розмір простору їх допустимих значень для досягнення періоду ПВП $T = M$ у $M/\varphi(M)$ разів. Швидкість роботи розробленого генератора перевищує швидкість роботи генератора перестановок на основі ГПВЧ LFIB78 із застосуванням алгоритму Фішера-Йєтса для $M \le 125$ (зокрема, для $M = 20$ – у 2,1 рази; $M = 50$ – у 1,6 рази; $M = 100$ – у 1,2 рази);

− розроблено структурну схему та алгоритм роботи пристрою двоконтурного криптографічного перетворення даних, що забезпечують можливість його практичної реалізації і 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 в $2^{4n} \cdot (n!)^2$ разів, де n – розрядність блоку даних;

− розроблено методику вибору параметрів первинних генераторів перестановок для комбінаційного генератора з комбінаційною функцією підсумовування за модулем M, 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;

– 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. Застосування розроблених критеріїв дозволило виявити статистичні відхилення для деяких генераторів ПВП, які успішно проходять усі автокореляційні тести пакету TestU01, а також для реалізації квантового ГВЧ.

Результати досліджень знайшли практичне застосування 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); Департаменті освіти та гуманітарної політики Черкаської міської ради (система обліку кадрів, м. Черкаси), а також використані в навчальному процесі Черкаського державного технологічного університету, Черкаського інституту пожежної безпеки імені Героїв Чорнобиля та Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

Особистий внесок здобувача. Дисертація є самостійно виконаною завершеною працею здобувача. Наукові положення і практичні результати, що в ній містяться та виносяться на захист, отримані автором самостійно.

У роботах, опублікованих у співавторстві, автором: [3], [36], [54] – розроблено та досліджено метод комбінованого факторіального кодування інформації; [4] – розроблено метод і критерій оцінювання якості послідовностей випадкових чисел; [6] – розроблено метод факторіального кодування з заданим числом інверсій; [7], [14] – досліджено статистичні властивості послідовностей комбінаційного генератора; [8], [12], [37] – запропоновано використати підхід до виділення комбінаційної частини та пам'яті в структурі пристрою формування залишку; [9] – розроблено метод організації ключового обміну; [10] – виконано дослідження кореляційних властивостей послідовностей; [11] – досліджено ізоморфізм графів ЛКГ та циклічної групи в $\mathbb{Z}_M$ з операцією множення; [13], [15] – виконано розробку генератора ПВП; [16] – сформульовано правила визначення кількості нуль-циклів у графі станів ЛКГ; [17] – розроблено та досліджено критерій оцінювання точності відтворення закону розподілу д.в.в.; [18] – визначено засоби захисту інформації для дистанційної навчальної системи; [19], [38] – запропоновано принципи формування основної матриці стохастичного генератора; [20] – теоретично обґрунтовано підхід до формування ПВП підвищеної розрядності; [21], [39] – запропоновано підхід та розроблено метод двоконтурного криптографічного перетворення інформації; [22] – розроблено метод підвищення стійкості електронних кодових замків; [23], [49] – розроблено та застосовано алгоритм дослідження рівномірності розподілу псевдовипадкових послідовностей у k-вимірному просторі; [24], [40] – розроблено та досліджено метод формування випадкової послідовності перестановок; [26], [50] – виконано аналіз ефективності використання операції суми за модулем в якості

комбінаційної функції; [27], [31] – запропоновано методику дослідження псевдовипадкових послідовностей; [55] – формалізовано алгоритм побудови псевдовипадкової послідовності; [28], [41], [51] – розроблено та досліджено метод формування імітовставки; [29] – виконано дослідження коефіцієнтів автокореляції випадкових послідовностей чисел; [30] – запропоновано методику оцінки статистичних характеристик ПВП; [35], [42], [52], [56], [59] – розроблено та досліджено метод повного факторіального кодування інформації; [43], [44] – досліджено методи формування ПВП; [45], [57] – розроблено та досліджено метод факторіального кодування з відновленням даних за перестановкою; [46], [47] – розроблено та досліджено метод і пристрій факторіального кодування з виявленням і виправленням помилок; [48], [60] – досліджено топологію ЛКГ. З робіт, опублікованих у співавторстві, для вирішення задач, поставлених у дисертаційному дослідженні, використано результати, отримані здобувачем особисто.

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи докладалися і обговорювалися на XI, XVI Міжнародній науково-технічній конференції «Системний аналіз та інформаційні технології» (Київ, 2009, 2014); II Міжвузівській науково-практичній конференції «Актуальні проблеми технічних і природних наук у забезпеченні цивільного захисту» (Черкаси, 2009); Міжнародній науково-практичній конференції «Інформаційні технології та комп'ютерна інженерія» (Вінниця, 2010); Науково-технічній конференції «Проблеми телекомунікацій» (Київ, 2011); V Міжнародній науково-технічній конференції «Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування» (Вінниця, 2011); Міжнародній науково-практичній конференції «Інформаційні технології в освіті, науці і техніці» (Черкаси, 2012); Міжнародній науковій конференції «Информационные технологии и системы» (Мінськ, Білорусь, 2012); Міжнародній науково-практичній інтернет-конференції «Сучасність, наука, година. Взаємодія та взаємовплив» (Київ, 2012); Всеукраїнській науково-практичній Internet-конференції «Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку» (Черкаси, 2013-2017); Міжнародній науково-практичній конференції «Обробка сигналів і негауссівських процесів» (Черкаси, 2013); IX Міжнародній науковій конференції «Сучасні досягнення в науці і освіті» (Нетанія, Ізраїль, 2014); Doctoral Summer School (Berlin, Germany, 2015); II, III, IV, V Міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси, 2014, 2015, 2016, 2017); International Scientific Conference «The scientific potential of the present» (St. Andrews, Scotland, UK, 2016); Всеукраїнській науково-практичній конференції «Актуальні задачі та досягнення у галузі кібербезпеки» (Кропивницький, 2016).

Публікації. Основний зміст, наукові положення та результати дисертаційного дослідження викладено в 80 наукових працях, основні 60 з яких наведено в авторефераті, в тому числі: 2 розділи в колективних монографіях [1], [2], 4 наукові статті у виданнях, що входять до наукометричних баз даних Scopus та / або Web of Science [3]–[6], 2 наукові статті в фахових виданнях інших країн [7], [35] та 27 статей у наукових виданнях, що входять до переліку МОН України та інших

наукометричних баз даних [8]–[34], 12 патентів України [36]–[47] та 13 матеріалів і тез доповідей наукових конференцій [48]–[60].

Структура і об'єм дисертаційної роботи. Дисертаційна робота складається з анотації, 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. Робота містить 104 таблиці та 80 рисунків.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЙНОЇ РОБОТИ

У вступі обґрунтовано актуальність та доцільність теми дисертаційного дослідження, сформульовано мету та задачі дослідження, визначено об'єкт, предмет і методи досліджень, представлено наукову новизну та практичну цінність отриманих результатів, зазначено зв'язок роботи з науковими програмами, планами та темами, наведено відомості щодо апробації, публікації та застосування результатів дослідження.

Перший розділ містить результати аналізу існуючих підходів, методів і засобів, що реалізують сумісний захист інформації від помилок каналу зв'язку, несанкціонованого доступу та/або модифікації даних, а також методів формування й оцінювання ПВП.

Аналіз існуючих методів формування послідовностей перестановок свідчить про їх обмежену ефективність, пов'язану з необхідністю приведення випадкового числа додаткового ГПВЧ до діапазону зі змінною верхньою межею, що, в свою чергу, призводить до збільшення розрядності цього ГПВЧ з метою усунення нерівномірності розподілу перестановок. Сформульовано задачу роботи, що полягає в удосконаленні методу формування випадкових послідовностей перестановок, частково або повністю позбавленого вказаних недоліків. У основі нового методу передбачено використання ФСЧ.

Показано доцільність інтегрованого вирішення задач криптографії та завадостійкого кодування. Встановлено, що відома методологія інтеграції процесів завадостійкого кодування та шифрування даних на основі досконалих алгебраїчних конструкцій не забезпечує захист від несанкціонованої модифікації інформації й обмежена застосуванням у широкосмугових системах зв'язку. Інші відомі методи, що інтегрують у собі процеси завадостійкого кодування, забезпечення цілісності та/або конфіденційності інформації, мають недоліки, які ускладнюють їх практичну реалізацію. Водночас використання перестановок і ФСЧ для зазначених цілей є перспективним напрямом досліджень. Визначено наступну задачу дисертаційної роботи, що полягає в розробці методів забезпечення захисту інформації на основі роздільного та нероздільного факторіального кодування даних.

Аналіз властивостей найпростіших генераторів ПВП – ЛКГ і генератора на основі регістра зсуву з лінійними зворотними зв'язками (РЗЛЗЗ) – свідчить про їх обмеження з огляду на необхідність підбору параметрів для забезпечення заданих статистичних властивостей ПВП. Показано, що на цей час недостатньо вивченими є

питання, пов’язані з формуванням на основі ЛКГ послідовностей, що складаються з усіх цілих чисел діапазону $[0;M-1]$, (перестановок порядку M) шляхом послідовного обходу вузлів графа його станів. Сформульовано задачу роботи, яка полягає в дослідженні топології графів станів ЛКГ і розвитку методу побудови ГПВЧ на основі конкатенації зв’язних компонентів графа ЛКГ.

Аналіз методів підвищення якості ПВП на основі їх комбінації показує, що ПВП, сформовані комбінаційним генератором з комбінаційною функцією підсумовування за модулем, успішно проходять відомі пакети тестування, проте теорія побудови таких генераторів у літературі висвітлена недостатньо. З огляду на це сформульовано задачу дисертаційного дослідження, що полягає в обґрунтуванні принципів побудови комбінаційних генераторів ПВП з комбінаційною функцією підсумовування за модулем.

Сформульовано вимоги, що пред’являються до ГПВЧ. Виконано аналіз методів і засобів оцінювання послідовностей випадкових чисел. Показано, що одним із найпоширеніших тестів, що дозволяє виявити статистичні нерегулярності досліджуваних послідовностей чисел, є автокореляційний тест. У той же час, питання оцінки коефіцієнтів автокореляції все ще недостатньо вивчене. Тому задачами дисертаційного дослідження є удосконалення критерію комплексного оцінювання бічних пелюсток автокореляційної функції (АКФ) і розробка методу оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, що дозволяє виявити статистичні нерегулярності, які не виявляються існуючими методами тестування.

Відсутність формалізованого механізму використання принципів, методів і моделей роздільного та нероздільного факторіального кодування, а також методів і моделей формування для нього ключових послідовностей вимагає розроблення методології захисту інформації на основі факторіального кодування, що є заключною задачею дисертаційної роботи.

Другий розділ містить результати наукових досліджень, пов’язаних із розробкою методу формування випадкових послідовностей перестановок на основі ФСЧ, методів захисту інформації від нав’язування хибних даних і помилок каналу зв’язку на основі роздільного факторіального кодування, а також математичної моделі процесу декодування роздільних факторіальних кодів.

Розроблено метод формування випадкових послідовностей перестановок, який базується на використанні ФСЧ для представлення синдрому перестановки S_F. Формування кожної наступної перестановки зводиться до модифікації її синдрому відповідно до ітераційного виразу:

$$S_F(j) = f\left(S_F(j-1)\right) \dot{+} t_{10}(j), \qquad (1)$$

де $f\left(S(j-1)\right)$ – функція від значення синдрому попередньої перестановки; $t_{10}(j)$ – випадкове число в десятковій системі числення, що позначає зсув порядкового номеру перестановки відносно модифікованого номеру попередньої перестановки на відрізку $[0, M!-1]$. Випадкову величину $t_{10}(j)$ формує вбудований генератор

випадкових / псевдовипадкових чисел; символ $\dot{+}$ позначає додавання чисел різних систем числення – факторіального $\left(f\left(S_F\left(j-1\right)\right)\right)$ та десяткового $\left(t_{10}\left(j\right)\right)$. Розроблено правила додавання цих чисел.

Запропоновано реалізації методу для різних процедур обчислення синдрому наступної перестановки: з фіксованим нулем, з випадковим нулем, з модифікованим випадковим нулем. Передбачено два режими формування послідовності перестановок – відкритий і прихований.

Технічний результат застосування запропонованого методу може бути досягнутий за допомогою пристрою, структурна схема якого показана на рис. 1.

Реалізація пристрою дозволяє формувати випадкову послідовність перестановок, уникнути приведення випадкового числа до потрібного діапазону, зменшити розрядність внутрішнього стану додаткового ГПВЧ не менш ніж на $\log_2 M$ біт, а також підвищити швидкість формування перестановок порівняно з алгоритмом Фішера-Йєтса (зокрема, для $M=5$ – у 2,1 рази; $M=10$ – у 2,6 рази; $M=20$ – у 2,8 рази).

Рис. 1. Структурна схема пристрою формування випадкових послідовностей перестановок

Розроблено метод повного факторіального кодування інформації на основі використання перестановки в якості перевірної частини кодового слова. Цей метод передбачає перетворення символів повідомлення на послідовність взаємопов'язаних чисел у ФСЧ, а також формування перестановки у відповідності з секретним ключем після обробки останнього символу повідомлення. Це дозволяє формувати самосинхронізований («без коми») код виявлення модифікацій повідомлення.

Досліджено статистичні властивості контрольної суми ПФК в залежності від способу її формування. Показано, що ймовірність зламу ПФК методом грубої сили $P_{ПС}\left(FFC\right)\le\left(M!\right)^{-3}$.

Спрощену структурну схему кодера та декодера ПФК показано на рис. 2.

Розроблено математичну модель процесу декодування ПФК. Визначено оцінку ймовірності не виявленої декодером ПФК (FFC) помилки $P_{ud}\left(FFC,p_0\right)$ для двійко-

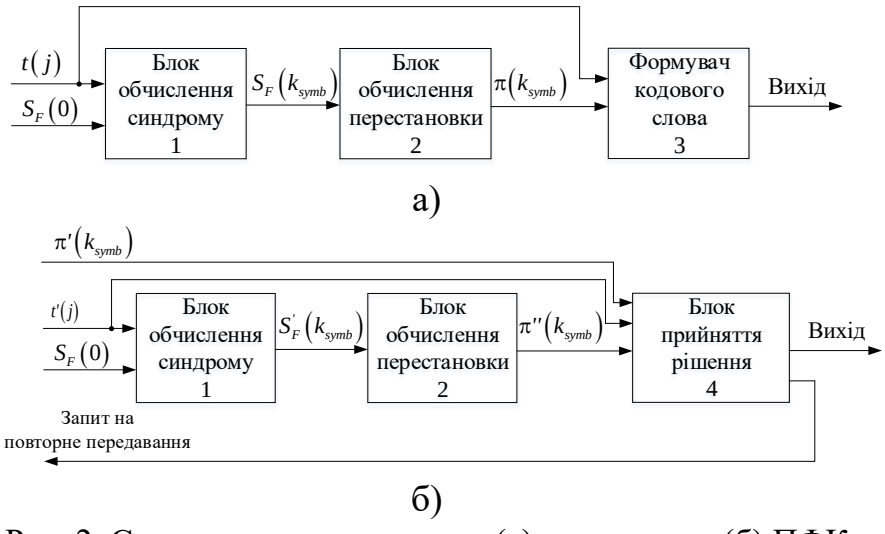


Рис. 2. Структурна схема кодера (а) та декодера (б) ПФК

вого симетричного каналу з перехідною ймовірністю p_0, $q_0 = 1 - p_0$.

Нехай k і r – число двійкових символів у інформаційній $A(x)$ і перевірній $R(x)$ частинах кодового слова, $n = k + r$ – його повна довжина. Тоді для $M! < 2^k$ і сюр'єктивного відображення $A(x) \to R(x)$ імовірність не виявленої декодером ПФК помилки оцінюється виразом $P_{ud}(FFC, p_0) = \left[\left(1 - q_0^k\right)/M!\right] \cdot p_r$, де p_r – імовірність появи помилки, здатної перетворити представлену в двійковому вигляді перестановку $R(x)$ у будь-яку з $M!$ можливих перестановок.

Нехай символи перестановки кодуються рівномірним кодом. Тоді $r = l_r \cdot M$, де $l_r = \lceil \log_2 M \rceil$. Позначимо через $f_{per}(i)$ кількість помилок ваги $i \in [0; r]$, здатних перетворити перестановку $R(x)$ у перестановку.

Теорема 10. Імовірність p_r визначається виразом

$$p_r = \sum_{i=0}^{\lfloor r/2 \rfloor} f_{per}(2i)\, p_0^{2i} q_0^{r-2i}, \tag{2}$$

де $\sum_{i=0}^{\lfloor r/2 \rfloor} f_{per}(2i) = M!$, $f_{per}(0) = 1$, $f_{per}(2) \le l_r \cdot M/2$, $f_{per}(4) \le l_r \cdot M \cdot \left(l_r \cdot (M+8) - 10\right)/8$.

Теорема 11. Для $\log_2 M \in \mathbb{Z}$ справедлива рівність $f_{per}(i) = f_{per}(r - i)$.

Приймемо $p_r = \sum_{i=0}^{m_1} f_{per}(2i)\, p_0^{2i} q_0^{r-2i} + \Delta_{per}(m_1)$, де $\Delta_{per}(m_1) = \sum_{i=m_1+1}^{\lfloor r/2 \rfloor} f_{per}(2i)\, p_0^{2i} q_0^{r-2i}$.

Для ймовірності $\Delta_{per}(m_1)$ має місце оцінка:

$$\Delta_{per}(m_1) \le e^{-\lambda} \cdot \left(\lambda^{2(m_1+1)} / \left(2(m_1+1)\right)!\right) \cdot \left((2m_1+3)^2 / \left((2m_1+3)^2 - \lambda^2\right)\right), \tag{3}$$

де $\lambda = r \cdot p_0$ і $m_1 > (\lambda - 3)/2$.

Значення m_1 вибирається таким чином, щоб $\Delta_{per}(m_1) \le \varepsilon_1$.

Для $M! \ge 2^k$ та ін'єктивного або бієктивного відображення $A(x) \to R(x)$ $P_{ud}(FFC, p_0) = \left(1 - q_0^k\right)/\left(2^k - 1\right) \cdot p_r^*$, де p_r^* – імовірність появи ненульової помилки, здатної перетворити перестановку $R(x)$ у будь-яку з $\left(2^k - 1\right)$ інших дозволених перестановок.

Теорема 12. Імовірність p_r^* визначається виразом

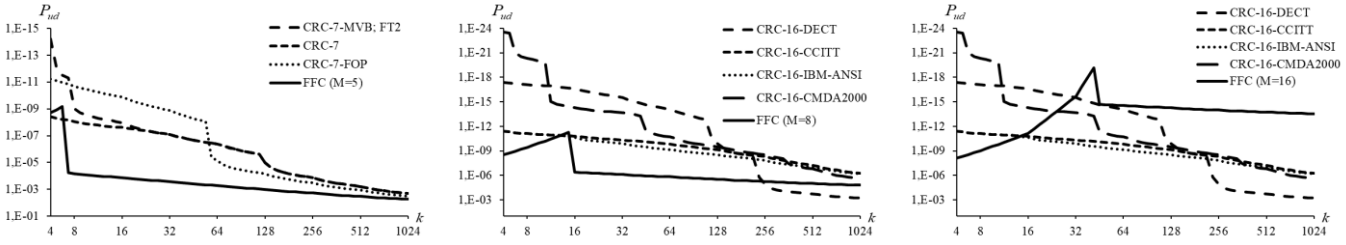
$$p_r^* = \sum_{i=1}^{\lfloor r/2 \rfloor} f_{per}^*(2i)\, p_0^{2i} q_0^{r-2i}, \tag{4}$$

де $\sum_{i=1}^{\lfloor r/2 \rfloor} f_{per}^*(2i) = 2^k - 1$ і $f_{per}^*(i) \le f_{per}(i)$, звідки слідує:

$$p_r^* \le \sum_{i=1}^{m_1} f_{per}(2i)\, p_0^{2i} q_0^{r-2i} + \Delta_{per}(m_1). \tag{5}$$

Відповідно до рис. 3, ПФК за рахунок властивості циклової самосинхронізації дозволяє забезпечити близьку до CRC-коду ефективність виявлення помилок (для $k=1024$ і $p_0=10^{-3}$ різниця між енергетичними виграшами CRC-коду і ПФК становить $\Delta P_{CRC-7}-\Delta P_{FFC-15}\le 0.384\,дБ$; $\Delta P_{CRC-16}-\Delta P_{FFC-24}\le 0.811\,дБ$), а в деяких випадках і перевищити її ($\Delta P_{CRC-16-DECT}-\Delta P_{FFC-24}=-1.089\,дБ$).

ПФК є забезпечує більшу достовірність порівняно зі спільним використанням у одному блоці даних імітовставки, перевірної частини CRC-коду і прапору циклової синхронізації. Так, наприклад, для $r_{MAC}=40$, $k\ge 32$ і $p_0=10^{-3}$ справедливо: $\Delta P_{CRC-16}-\Delta P_{FFC-64}\le -0.032\,дБ$ для $k=32$ і $\Delta P_{CRC-16}-\Delta P_{FFC-64}\le -2.683\,дБ$ для $k=1024$. Для $r_{FFC}=24$ ефективність використання ПФК зростає.

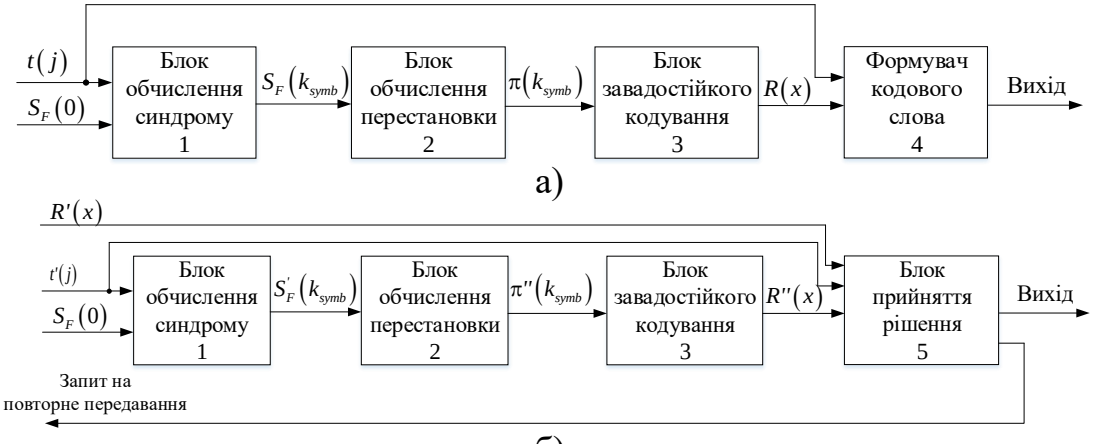


а) б) в)

Рис. 3. Графіки залежностей оцінок імовірності невиявленої помилки від довжини інформаційної частини кодового слова для $p_0=10^{-3}$ і $r_{CRC}=7$, $r_{FFC}=15$ (а); $r_{CRC}=16$, $r_{FFC}=24$ (б); $r_{CRC}=16$, $r_{FFC}=64$ (в)

Розроблено метод комбінованого факторіального кодування інформації на основі використання контрольної суми CRC-коду в якості перевірної частини кодового слова. Контрольна сума CRC-коду обчислюється за образом інформаційної частини, сформованим відповідно до принципів ПФК. Це дозволяє формувати код виявлення модифікацій повідомлення довільної довжини, що має високу стійкість до зламу.

Спрощена структурна схема кодера та декодера КФК показана на рис. 4.



а)

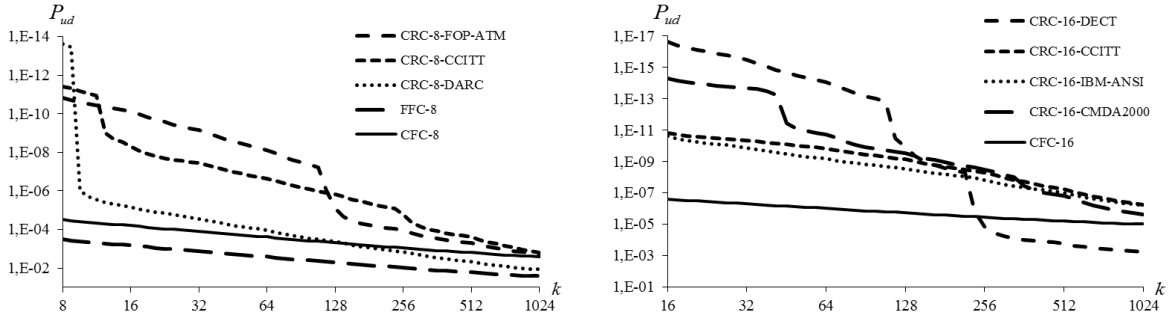
б)

Рис. 4. Структурна схема кодера (а) та декодера (б) КФК

Імовірність зламу КФК методом грубої сили $P_{IIC}\left(CFC\right)\le\left(M!\right)^{-3}\cdot\left(N_{r_{CFC}}\right)^{-1}$, де $N_{r_{CFC}}$ – кількість можливих утворюючих CRC-код багаточленів степені r_{CFC}.

Виявляюча здатність КФК в цілому поступається виявляючій здатності CRC-коду, однак для деяких утворюючих поліномів CRC-коду і довжини інформаційної частини справедливо $\Delta P_{CFC}>\Delta P_{CRC}$. Так, наприклад, виходячи з рис. 5, $\Delta P_{CFC-8}>\Delta P_{CRC-8-DARC}$ для $k\ge146$ ($\Delta P_{CRC-8-DARC}-\Delta P_{CFC-8}\approx-0.638\,дБ$ для $k=1024$), а $\Delta P_{CFC-16}>\Delta P_{CRC-16-DECT}$ для $k\ge243$ ($\Delta P_{CRC-16-DECT}-\Delta P_{CFC-16}\approx-1.219\,дБ$ для $k=1024$).

Водночас КФК забезпечує більшу достовірність порівняно зі спільним використанням у одному блоці імітовставки та перевірної частини CRC-коду – наприклад, для $r_{MAC}=8$, $k=1024$ і $p_0=10^{-3}$ $\Delta P_{CRC-8}-\Delta P_{CFC-16}\le-1.573\,дБ$.



а) б)

Рис. 5. Графіки залежностей оцінок імовірності невиявленої помилки від довжини інформаційної частини кодового слова для $p_0=10^{-3}$ і $r_{CFC}=8$ (а); $r_{CFC}=16$ (б)

Розроблено метод факторіального кодування інформації з проріджуванням на основі використання контрольної суми ПФК в якості перевірної частини кодового слова. За рахунок того, що контрольна сума ПФК обчислюється за частиною $\left(k_{FCD}\right)$ інформаційних символів, що поступають на вхід кодера, цей метод дозволяє формувати самосинхронізований код виявлення модифікацій повідомлення і скоротити в порівнянні з повним факторіальним кодуванням час формування кодового слова і об’єм використовуваної пам’яті.

Імовірність зламу факторіального коду з проріджуванням (ФКП) грубою силою $P_{IIC}\left(FCD\right)\le\left(C_k^{k_{FCD}}\right)^{-1}\cdot\left(M!\right)^{-3}$. Виявляюча здатність ФКП поступається виявляючій здатності ПФК.

Розроблено метод роздільного факторіального кодування інформації з декількома контрольними сумами на основі використання в якості перевірної частини кодового слова конкатенації контрольних сум ПФК, кожна з яких обчислюється за частиною інформаційних символів, які надходять на вхід кодера. Цей метод за рахунок паралельної обробки даних і одночасного формування декількох контрольних сум, що підлягають конкатенації, дозволяє створити самосинхронізований код виявлення модифікацій повідомлення, що володіє

високою стійкістю до зламу, та скоротити в порівнянні з ПФК час формування кодового слова і обсяг використовуваної пам’яті, а також зменшити вимоги до продуктивності кодека під час обчислення перестановок, що входять до складу кодового слова.

Розроблено структурну схему та алгоритм роботи кодека ФКДКСр.

Аналіз енергетичного виграшу ФКДКСр вказує на меншу виявляючу здатність ФКДКСр у порівнянні з ПФК за однакових швидкостей кодів. Імовірність зламу ФКДКСр (FCSCs) під час одноразової спроби підбору ключа

$$P_{IIC}\left(FCSCs\right) \le \left(\prod_{i=1}^{N} C^{k_{FCD}(i)}_{k-\sum_{j=1}^{i-1} k_{FCD}(j)} \cdot \left(M\left(i\right)!\right)^3 \right)^{-1}.$$

Третій розділ містить результати розробки та дослідження методів захисту інформації від несанкціонованого читання та помилок каналу зв’язку на основі нероздільного факторіального кодування, а також математичної моделі процесу декодування нероздільних факторіальних кодів.

Розроблено метод нероздільного факторіального кодування з відновленням даних за перестановкою шляхом бієктивного перетворення інформаційної послідовності у перестановку чисел деякого порядку. Параметри перетворення тримаються в таємниці. Метод дозволяє реалізувати єдину процедуру блокування несанкціонованого читання інформації та виявлення факту модифікації переданих даних за рахунок впливу помилок у каналі зв’язку.

Структурну схему кодера та декодера ФКВД представлено на рис. 6.

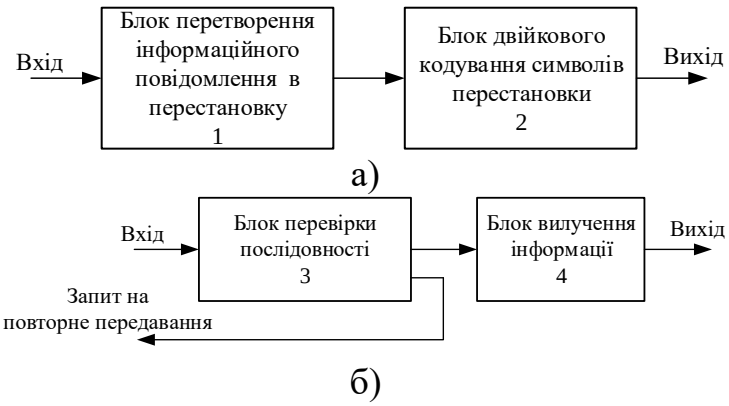


Рис. 6. Структурна схема кодера (а) та декодера (б) ФКВД

Визначено оцінку ймовірності не виявленої декодером помилки. За однакових швидкостей кодів для малих значень довжини інформаційного блоку k і кодування символів перестановок рівномірним двійковим кодом енергетичний виграш ФКВД перевищує відповідний енергетичний виграш ПФК і CRC-коду – для $p_0 = 10^{-3}$ відповідно до рис. 7 $\Delta P_{FCDR} - \Delta P_{FFC} \le 1.5 дБ$ $\left(k \le 18\right)$ і $\Delta P_{FCDR} - \Delta P_{CRC} \le 0.821 дБ$ $\left(k \le 15\right)$.

Подальше підвищення ефективності ФКВД може бути досягнуто шляхом доповнення інформаційного блоку додатковими перевірними бітами таким чином, щоб збільшення довжини блоку не призводило до зміни порядку перестановки. Це забезпечує підвищення достовірності переданих даних за рахунок існуючої надлишковості коду. Використання ФКВД з доповненням (ФКВДд) дозволяє

підвищити виявляючу здатність коду (наприклад, $\Delta P_{FCDRadd} - \Delta P_{FCDR} \approx 1.194 дБ$ для $k = 512$, $\Delta P_{FCDRadd} - \Delta P_{FCDR} \approx 1.601 дБ$ для $k = 1012$) і розширити діапазон значень розміру блоку даних k (з $k \le 18$ до $k \le 22$ для $p_0 = 10^{-3}$), для яких енергетичний виграш ФКВД перевищує відповідний енергетичний виграш ПФК.

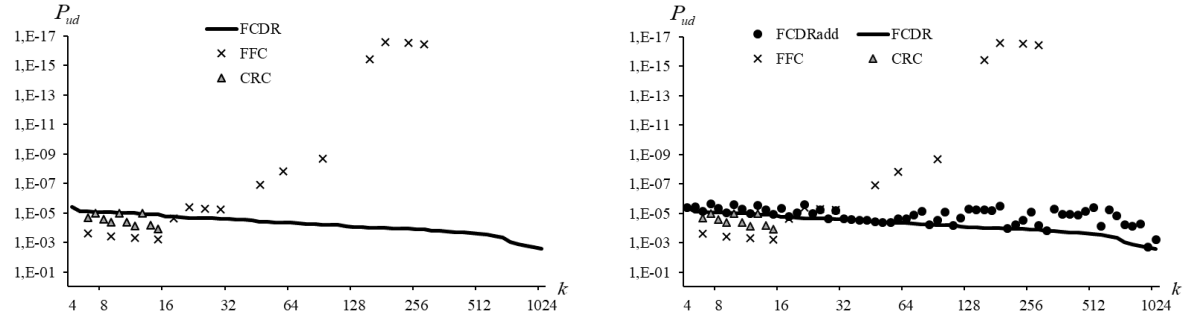


Рис. 7. Графіки залежностей оцінок імовірності невиявленої помилки від розміру блоку даних k для ФКВД, ПФК і CRC (а); ФКВДд, ФКВД, ПФК і CRC (б)

Розроблено метод нероздільного факторіального кодування інформації з декількома контрольними сумами на основі використання ФКВД. Кодове слово ФКДКСн формується шляхом конкатенації кодових слів ФКВД, кожне з яких обчислюється за частиною інформаційних символів. Цей код за рахунок паралельної обробки даних і одночасного формування декількох кодових слів, що підлягають конкатенації, дозволяє формувати самосинхронізований код довільної довжини, що володіє криптографічного стійкістю, скоротити в порівнянні з ФКВД час формування кодового слова і обсяг використовуваної пам'яті, а також зменшити вимоги до продуктивності кодека під час обчислення перестановок.

Розроблено структурну схему та алгоритм роботи кодека ФКДКСн.

Виявляюча здатність ФКДКСн не поступається виявляючій здатності ФКВД за однакових довжини інформаційного блоку k і швидкості коду.

Запропоновано метод факторіального кодування з заданим числом інверсій на основі ФКВД. Дозволена множина кодових слів формується з перестановок із числом інверсій, що належить заданому класу лишків. Це забезпечує підвищення достовірності передавання за рахунок збільшення кількості виявлених у кодовому слові помилок. Модуль класу лишків визначається виходячи з необхідного ступеня підвищення достовірності та допустимої втрати швидкості коду.

Показано, що вибором відповідного класу лишків для числа інверсій у перестановці можна вибрати потрібне значення енергетичного виграшу в обмін на втрату відносної швидкості передавання (наприклад (рис. 8), для $M = 8$ і $p_0 = 10^{-3}$ вибір класу лишків для модуля $q = 2$ забезпечує ймовірність невиявленої помилки на рівні $P_{ud}(FCGNI, p_0) = 7.24 \cdot 10^{-11}$ за швидкості коду $\nu_1 = 0.583$ (ці ж показники для ФКВД – $P_{ud}(FCDR, p_0) = 1.18 \cdot 10^{-5}$, $\nu_1 = 0.625$)).

Застосування ФКЗЧІ дозволяє збільшити енергетичний виграш нероздільного факторіального кодування порівняно з CRC-кодом за їх однакових швидкостей –

$0.986 дБ \le \Delta P_{FCGNI} - \Delta P_{CRC} \le 3.295 дБ$ для $p_0 = 10^{-3}$, $M = 8$ і максимальної швидкості в класі $B_M(q, R)$.

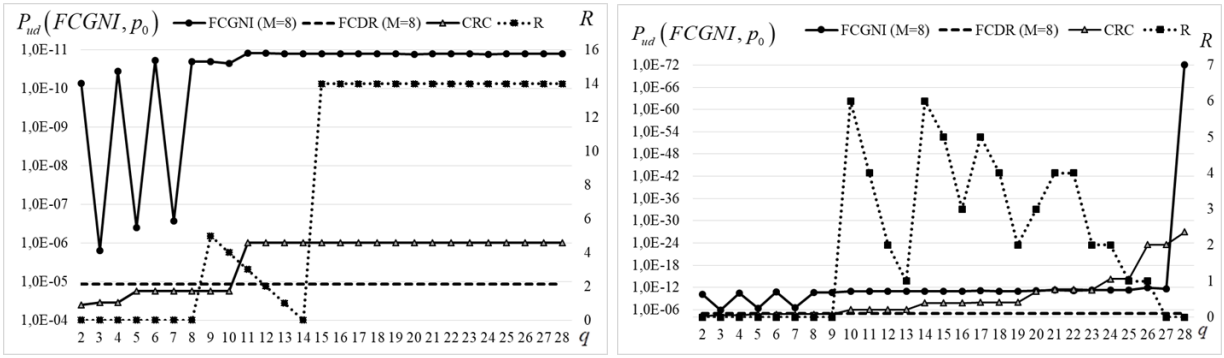


Рис. 8. Графіки залежностей оцінок імовірності не виявленої ФКЗЧІ помилки від модуля q для $M = 8$ і $p_0 = 10^{-3}$ та максимальної швидкості в класі $B_M(q, R)$ (а) і максимальної достовірності в класі $B_M(q, R)$ (б)

Структурна схема кодера ФКЗЧІ відповідає рис. 6а. Структурна схема декодера ФКЗЧІ наведена на рис. 9.

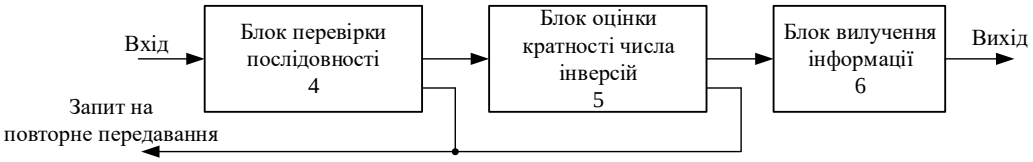


Рис. 9. Структурна схема декодера ФКЗЧІ

Запропоновано метод факторіального кодування інформації з виявленням і виправленням помилок. Для забезпечення можливості виправлення помилок кількість кодових слів, які використовуються для перенесення інформації, зменшується, а відстань між ними збільшується. Величина збільшення кодової відстані залежить від необхідного ступеня підвищення достовірності передавання інформації та допустимої втрати швидкості коду. Відстань між кодовими словами може визначатися, наприклад, як відстань Евкліда або Хеммінга. Показано, що виправлення помилок дозволяє підвищити відносну швидкість передавання ФКВД за рахунок зниження завадостійкості коду.

Встановлено також, що показники завадостійкості ФКВД і ФКВД з виправленням помилок (ФКВДвп) не є інваріантними відносно вибору сигнально-кодової конструкції, якщо в якості сигнальних векторів використовується деяка власна підмножина множини векторів усіх перестановок порядку M.

Розроблено структурні схеми та алгоритми роботи пристроїв кодування та декодування ФКВДвп.

Властивості всіх розроблених у рамках дисертаційного дослідження факторіальних кодів наведено в таблиці 1.

Таблиця 1

Властивості факторіальних кодів

Код	Роздільний	Завадостійкий		Крипто-стійкий	Іміто-стійкий	Само-синхронізується
		виявляє помилки	виправляє помилки			
ПФК	+	+	-	-	+	+
КФК	+	+	-	-	+	-
ФКП	+	+	-	-	-	+
ФКДКСр	+	+	-	-	+	+
ФКВД	-	+	-	+	-	+
ФКВДд	-	+	-	+	-	+
ФКДКСн	-	+	-	+	-	+
ФКЗЧІ	-	+	-	+	-	+
ФКВДвп	-	+	+	+	-	+

Сформульовано рекомендації щодо їх застосування.

Розроблені методи факторіального кодування передбачають використання генератора перестановок для формування ключової перестановки, організації систем з множинним доступом (ФКЗЧІ), забезпечення розсіювання та рандомізації (ФКВД). У свою чергу, використання для цих цілей розробленого методу формування перестановок на основі ФСЧ потребує додаткового генератора рівномірно розподілених у діапазоні $[0, M!-1]$ випадкових чисел.

Четвертий розділ містить результати наукових досліджень, пов'язаних із аналізом топології графа станів ЛКГ, вдосконаленням методу формування ПВП на основі конкатенації зв'язних компонентів графа станів ЛКГ для генерації елементів перетворення інформації в процесі факторіального кодування, а також удосконаленням методу симетричного криптографічного захисту інформації для забезпечення її конфіденційності.

На основі теорії монад і їх графів побудовано типові структури графа станів ЛКГ. За В. І. Арнольдом під монадою розуміємо відображення скінченної множини в себе; вершинами графа монади є всі елементи цієї скінченної множини, а орієнтовані ребра з'єднують кожен елемент з його образом у результаті відображення. Кожна зв'язна компонента графа монади є лісом з орієнтованих до коріння кореневих дерев, коріння яких з'єднані орієнтованим циклом.

Нехай S – скінченна група, а відображення $f: S \to S$ перетворює кожен її елемент $s \in S$ відповідно до математичної моделі ЛКГ: $f(s) = |K \cdot s + C|_M$, де K, C, M – параметри ЛКГ. У роботі досліджено та представлено структури графів монад групи S ЛКГ для всіх можливих параметрів з $M \le 20$. Водночас введено такі позначення графів: O_n – орієнтований цикл з n вершин; A_n – зв'язний граф з $2n$ вершин, який є циклом довжини n, оснащеним n одноребернимими деревами, що входять по одному в кожну з n вершин циклу; T_{2^n} – кореневе дерево з $2n$ вершинами і n поверхами крім кореня, що розгалужується бінарно на поверхах

$1,\ldots,n-1$ (корінь вважається нульовим поверхом, і в нього теж входять два ребра: одне – від нього самого і одне – від єдиної вершини першого поверху); E_n – кореневе дерево з n вершинами, з кожної з яких ребро веде прямо в корінь $\left(E_2 = A_1 = T_2\right)$; D_n – $4n$-вершинний граф, що складається з циклу O_n довжини n, оснащеного в кожній своїй вершині трьома вхідними до неї ребрами $\left(D_1 = E_4\right)$.

Виконано узагальнення проаналізованих структур, представлено типові графи ЛКГ. Параметри, характерні для деяких з типових графів:

1) O_M – для:
   а) $M \geq 2,\ K = 1,\ C = 1;$
   б) $M = 2^p,\ K = 4l+1,\ C = 2m+1,\ l,m \in \mathbb{Z} \geq 0;$
   в) M – простого, $K = 1,\ C \geq 1;$
2) dO_t – для $M = 2^p,\ K = 4l-1,\ l \in \mathbb{Z} \geq 1$, і $C = 2m+1,\ m \in \mathbb{Z} \geq 0$. За такої умови:
   а) для $l = 2^{k-2}\ \left(K = 2^k - 1\right),\ k \geq 2$, має місце $t = 2^{p-l+1},\ d = 2^{l-1};$
   б) для $l = 2k-1\ \left(K = 8k-5\right),\ k \geq 1$, має місце $t = M/2$ і $d = 2;$
   в) для $l = 2k, k \geq 1, K \neq 2^r - 1,\ r \geq 3$ $(k \neq 2^{r-3}:\ k = 2^{i-4}\left(2j+1\right)$, а $l = 2^{i-3}\left(2j+1\right)$ для $j \in \left[1; 2^{p-i}-1\right],\ i \in \left[4; p-1\right]$) має місце $t = M/2^{i-2},\ d = 2^{i-2};$
3) $dO_t + O_1$ – для M – простого, $K \geq 2,\ C \in \mathbb{Z};$
4) дерево з коренем O_1 – для $M = 2^p,\ K \in \left\{2l : l \in \mathbb{N}, 0 < l < 2^{p-1}\right\},\ C \in \left\{0,1,\ldots,2^p - 1\right\}$.

Аналіз топології ЛКГ показує, що ніяких складніших структур, крім добутків дерев і циклів, у графах монад $f : S \to S$ не зустрічається: граф ЛКГ є незв'язним об'єднанням циклів, оснащених добутками дерев. Оскільки $E_n = T_{n^1} * O_1,\ A_t = T_{2^1} * O_t,$ $D_t = T_{4^1} * O_t$, то кожну зв'язну компоненту графа ЛКГ можна представити у вигляді $T_{a^n} * \left(T_{b^m} * O_t\right)$. Тоді узагальнений граф станів ЛКГ описується виразом:

$$G_{LCG} = \sum_{i=1}^{d} d_i \left(T_{a_i^{n_i}} * \left(T_{b_i^{m_i}} * O_{t_i}\right)\right), \tag{6}$$

де d – число різних типів компонент зв'язності графа станів ЛКГ;

d_i – число компонент зв'язності графа станів ЛКГ i-го типу;

$a_i,\ n_i,\ b_i,\ m_i,\ t_i$ – параметри компонент зв'язності графа станів ЛКГ i-го типу.

За цих умов $\sum_{i=1}^{d} d_i a_i^{n_i} b_i^{m_i} t_i = M$.

Виконано дослідження впливу параметрів ЛКГ на його топологію. Для цього досліджено графи ЛКГ і циклічної групи в $\mathbb{Z}_M$ з операцією множення для простого M. Сформульовано і доведено наступну теорему.

Теорема 1. Кожна відмінна від O_1 компонента зв'язності графа ЛКГ з параметрами K, C і простим модулем M ізоморфна графу циклічної групи $\langle K \rangle$ в $\mathbb{Z}_M$ з операцією множення і породжувальним елементом K, $1 < K < M$.

Визначено властивості, що характеризують залежність порядку циклічної групи від породжувального елемента K. Сформульовано і доведено наступні теореми, що визначають умови існування і кількість циклів O_1 у графі станів ЛКГ.

Теорема 2. Точка $s_0 = 0$ є циклом O_1 у графі станів ЛКГ тоді і тільки тоді, коли $C = 0$.

Теорема 3. Для існування циклу O_1 у графі станів ЛКГ необхідно і достатньо, щоб значення C було кратне $НСД(K-1, M)$.

Теорема 4. Кількість циклів O_1 у графі станів ЛКГ дорівнює $e = НСД(K-1, M)$ (для $|C|_e = 0$).

Зауваження 1. Для $K = 1$ і $C \neq 0$ граф станів ЛКГ не містить жодного циклу O_1. У цьому випадку граф станів ЛКГ містить $d = НСД(M, C)$ циклів довжиною $t = M / НСД(M, C)$.

Зауваження 2. Для $K = 1$ і $C = 0$ граф станів ЛКГ завжди містить M циклів O_1.

Теорема 5. Максимальна кількість циклів O_1 у графі станів ЛКГ з параметрами M і $K > 1$ досягається для $K = Mk/p + 1$ і $C = Mc/p$, де p – мінімальний множник в розкладанні числа M на прості множники, k і c – будь-які цілі числа, що задовольняють умовам $1 \le k < p$ і $0 \le c < p$.

Теорема 6. Граф станів ЛКГ з параметром M не має циклів O_1 тоді і тільки тоді, коли:

1) $C \neq 0$ для $K = 1$;

2) $e = НСД(K-1, M) > 1$ і $|C|_e \neq 0$ для $K > 1$.

Сформульовано методику вибору параметрів ЛКГ, граф станів якого не має циклів O_1. Наведено приклади її реалізації.

Теорема 7. Граф станів ЛКГ з параметром M має один цикл O_1 тоді і тільки тоді, коли $e = НСД(K-1, M) = 1$.

Наведені властивості топології ЛКГ дозволяють спростити процедуру визначення параметрів ЛКГ з необхідною структурою графа його станів і істотно (більше, ніж удвічі) скоротити обсяг обчислень.

Виходячи з результатів дослідження топології ЛКГ, удосконалено метод формування ПВП на основі лінійного конгруентного методу, який за рахунок конкатенації не тільки відокремлених і непересічних циклів у графі станів ЛКГ, а й передциклів (дерев), якщо вони в ньому містяться, дозволяє формувати ПВП рівномірно розподілених на відрізку $[0; M-1]$ чисел. Удосконалення методу дозволяє збільшити розмір простору допустимих значень параметрів ЛКГ для досягнення періоду ПВП $T = M$ у $M/\varphi(M)$ разів.

Розроблено структурну схему та алгоритм роботи пристрою формування ПВП на основі ЛКГ з будь-якою структурою графа його станів, що забезпечують можливість його практичної реалізації та дозволяють мінімізувати часові витрати на вибір параметрів ЛКГ.

Швидкість роботи розробленого генератора перевищує швидкість роботи генератора перестановок із застосуванням алгоритму Фішера-Йєтса на основі ГПВЧ:

- LFIB78 – для порядку перестановки $M \le 125$ (зокрема, для $M = 20$ – у 2,1 рази; $M = 50$ – у 1,6 рази; $M = 100$ – у 1,2 рази);
- MarsaLFIB4 – для порядку перестановки $M \le 142$ (зокрема, для $M = 20$ – у 2,4 рази; $M = 50$ – у 1,9 рази; $M = 100$ – у 1,4 рази);
- DX-47-3 – для порядку перестановки $M \le 135$ (зокрема, для $M = 20$ – у 2,3 рази; $M = 50$ – у 1,8 рази; $M = 100$ – у 1,3 рази).

Удосконалено метод симетричного криптографічного перетворення інформації на основі побітового додавання гами до символів відкритого тексту. Метод передбачає введення другого контуру шифрування, в якому кожне слово отриманого після першого контуру шифртексту у відповідності до ключа розщеплюється на два слова меншої розрядності. Отримані слова підсумовуються з числами, сформованими допоміжним ГПВЧ на основі ЛКГ. Результати підсумовування визначають номер рядка та стовпця для основної матриці генератора на основі ЛКГ. Параметри генератора тримаються в секреті та є частиною ключа. Сформоване генератором значення є символом шифртексту.

Удосконалений метод може бути реалізований у пристрої двоконтурного криптографічного перетворення, структурну схему якого наведено на рис. 10.

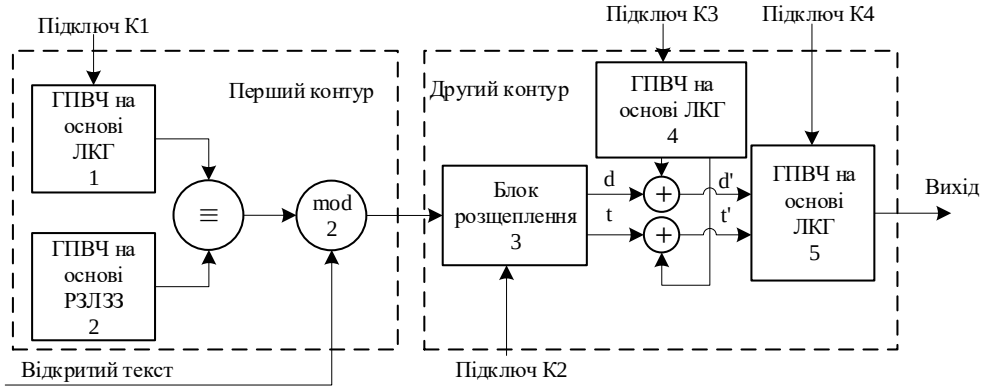


Рис. 10. Структурна схема пристрою двоконтурного криптографічного перетворення інформації

Результатом статистичного аналізу властивостей послідовностей на виході пристрою двоконтурного криптографічного перетворення даних за допомогою статистичних пакетів NIST STS, DIEHARD і TestU01 є успішне проходження всіх тестів, що свідчить про відповідність властивостей шифртексту властивостям випадкових послідовностей чисел. Таким чином, розроблений метод і пристрій, що його реалізує, дозволяють об’єднати переваги потокових і блокових шифрів: довжина ключа скінченна, трек помилки не перевищує довжини блоку, винесення ключа блокується, рандомізація інформаційного масиву не вимагається. Крім того, забезпечується підвищення криптографічної стійкості перетворення (або полегшуються вимоги до генератора гами) в порівнянні з використанням тільки першого контуру криптоперетворення.

П’ятий розділ містить результати дослідження комбінаційного методу формування ПВП на основі підсумовування за модулем.

Для вирішення цієї задачі виконано аналіз статистичних властивостей булевих перетворень д.в.в. X і Y. Аналіз показує, що рівномірно розподілену випадкову величину, придатну для застосування в криптографічних перетвореннях, можна отримати тільки для перетворень $X \oplus Y$ і $X \equiv Y$. Водночас статистичні властивості цих перетворень, застосованих до рандомізованих і нерандомізованих ПВП довільних періодів, породжуваних РЗЛЗЗ і ЛКГ, залежать від вектора початкового завантаження первинних генераторів і порядку обходу циклів. Тому застосування РЗЛЗЗ і ЛКГ у якості первинних джерел ПВП комбінаційного генератора є допустимим, проте потребує попередньої перевірки статистичних властивостей комбінацій.

Визначено закон розподілу д.в.в. на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем два слів, отриманих від групи з n первинних ГВЧ, розподіли яких мають відхилення від рівномірного закону. Показано, що за відхилень імовірностей появи нулів і одиниць для первинних генераторів на рівні $|\Delta_i| < 1/2$ відхилення ймовірностей появи нулів і одиниць на виході комбінаційного генератора зменшуються і досягають значення $2^{n-1}\prod_{i=1}^{n}|\Delta_i|$.

Визначено закон розподілу д.в.в. на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем M слів, отриманих від n первинних генераторів рівномірно розподілених випадкових чисел.

Приймемо спочатку $n = 2$. Нехай первинні випадкові величини $X \in [0, M_x - 1]$ і $Y \in [0, M_y - 1]$. Формована випадкова величина – $Z = |X + Y|_M$. Тоді закон розподілу функції Z має вигляд $P(Z = z_i) = \sum_{k=0}^{\lfloor (M_x + M_y - 2 - z_i)/M \rfloor} P(Z' = kM + z_i)$, де

$$P(Z' = z'_i) = \begin{cases} \dfrac{z'+1}{M_x M_y} \ \textit{для} \ z' \in [0, \min(M_x, M_y) - 1]; \\ \dfrac{1}{\max(M_x, M_y)} \ \textit{для} \ z' \in [\min(M_x, M_y) - 1, \max(M_x, M_y) - 1]; \\ \dfrac{M_x + M_y - z' - 1}{M_x M_y} \ \textit{для} \ z' \in [\max(M_x, M_y) - 1, M_x + M_y - 2]. \end{cases} \quad (7)$$

Теорема 8. Для рівномірного розподілу на множині цілих чисел потужності M д.в.в. $Z = |X + Y|_M$, достатньо, щоб хоча б одне зі значень M_x або M_y було кратне M.

Наслідок 1. Для рівномірного розподілу на множині цілих чисел потужності M д.в.в., отриманої в результаті підсумовування за модулем M групи з n незалежних д.в.в., рівномірно розподілених на множинах цілих чисел відрізків

$[0, M_i - 1]$, $i = 1, 2, \ldots n$, достатньо, щоб хоча б одне зі значень M_i було кратне M.

Наслідок 2. Достатньою умовою справедливості теореми 8 для д.в.в. X і Y з періодами T_x і T_y $\left(|T_x|_{M_x} = 0,\ |T_y|_{M_y} = 0\right)$ є умова взаємної простоти періодів T_x і T_y $\left(НСД\left(T_x, T_y\right) = 1\right)$.

Наслідок 3. Достатньою умовою справедливості наслідку 1 для n д.в.в. X_i, $i = 1, 2, \ldots n$, з періодами T_i $\left(|T_i|_{M_i} = 0\right)$ є умова попарної взаємної простоти періодів T_i, тобто $НСД\left(T_i, T_j\right) = 1$ для $\forall T_i, T_j$, $i \neq j$.

Теорема 9. Для рівномірного розподілу д.в.в. на множині цілих чисел потужності M на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем M слів від двох первинних генераторів, що циклічно формують деякі перестановки на множинах цілих чисел відрізків $[0, M_x - 1]$ і $[0, M_y - 1]$ для першого і другого генератора відповідно, достатньо, щоб M_x і M_y були взаємно прості і одне зі значень M_x або M_y було кратне M.

Наслідок 4. Для рівномірного розподілу д.в.в. на множині цілих чисел потужності M на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем M слів від групи з n незалежних первинних генераторів, кожний з яких циклічно формує перестановку на множині цілих чисел $[0, M_i - 1]$, $i = 1, 2, \ldots n$, достатньо, щоб значення M_i були попарно взаємно прості ($НСД\left(M_i, M_j\right) = 1$ для $\forall M_i, M_j$, $i \neq j$) і одне зі значень M_i було кратне M $\left(\exists M_j : |M_j|_M = 0\right)$.

На підставі наслідку 4 розроблено методику вибору параметрів первинних генераторів перестановок для комбінаційного генератора з комбінаційною функцією підсумовування за модулем M.

Успішно пройдено тестування ПВП комбінаційного генератора за допомогою: графічних тестів, аналізу розподілу символів у багатовимірному просторі, непараметричних критеріїв знаків і серій, тестів NIST STS, Diehard (кількість початкових таблиць перестановок для $M = 256$ і $\max\limits_i\left(M_i\right) = 256$ – 5 і більше, їх заповнення – адитивний, квантовий ГВЧ), тестів пакету TestU01 (із заповненням чотирьох первинних таблиць ЛКГ з $\max\limits_i\left(M_i\right) = 2^{32}$), кореляційного аналізу. Отримані результати підтверджують, що комбінаційний метод формування ПВП може бути використаний у задачах, які потребують високої якості ПВП. Можливість отримання рівномірного закону розподілу чисел на діапазоні з довільною верхньою межею дозволяє використовувати досліджуваний комбінаційний генератор в якості допоміжного ГПВЧ в пристрої формування випадкової послідовності перестановок на основі ФСЧ.

У **шостому розділі** дисертаційної роботи наведено результати наукових

досліджень, пов'язаних із розробкою методу і критеріїв кореляційного аналізу часових рядів для тестування ПВП з метою оцінювання їх статистичних відхилень, а також методології захисту інформації в телекомунікаційних системах і мережах на основі факторіального кодування даних.

Наведено інтегральну оцінку нормованих коефіцієнтів автокореляції (бічних пелюсток АКФ) $\rho_X(\tau)=M\left(\overset{\circ}{X}'\cdot\overset{\circ}{X}''\right)\Big/\sigma_X^2$ для $\tau\neq 0$, де $\overset{\circ}{X}'$ і $\overset{\circ}{X}''$ – центровані перерізи випадкового процесу в моменти часу t' і $t''=t'+\tau$, σ_X^2 – їх дисперсія. Показано, що за $n\to\infty$

$$n\sum_{\tau=1}^{\mathrm{T}}\rho_X^2(\tau)\to\chi_{\mathrm{T}}^2. \tag{8}$$

Оцінка (8) дозволяє створювати статистичні критерії перевірки кореляційних властивостей досліджуваних послідовностей за їх емпіричними оцінками. Для цього наведено перший і другий початкові моменти оцінок нормованих коефіцієнтів автокореляції для періодичної АКФ, АКФ непоповнюваної вибірки фіксованого розміру, що обчислюється за різними підходами (наприклад, за Anderson-Walker, Смірновим-Дуніним-Барковським або Kendall), АКФ «ковзного вікна» для послідовностей великого періоду. Уточнено дисперсію оцінок нормованих коефіцієнтів автокореляції

$$r_x(\tau)=\sum_{i=0}^{n-1-\tau}\left[\left(x_i-\bar{x}\right)\cdot\left(x_{i+\tau}-\bar{x}\right)\right]\Big/\sqrt{\sum_{i=0}^{n-1-\tau}\left(x_i-\bar{x}\right)^2\cdot\sum_{i=0}^{n-1-\tau}\left(x_{i+\tau}-\bar{x}\right)^2},$$

де $\bar{x}=\frac{1}{n}\sum_{i=0}^{n-1}x_i$ – статистична оцінка математичного сподівання:

$$D\left(r_x(\tau)\right)\le\frac{n^5-n^4(\tau+7)+n^3(7\tau+16)+n^2\left(2\tau^2-18\tau-12\right)-n\left(4\tau^2-16\tau\right)}{(n-1)^2(n-2)(n-3)(n-\tau)^2}. \tag{9}$$

Для нормально розподілених д.в.в. x_i вираз (9) має вигляд:

$$D_{норм}\left(r_x(\tau)\right)=\frac{n^4-(\tau+3)n^3+3\tau n^2+2\tau(\tau+1)n-4\tau^2}{(n+1)(n-1)^2(n-\tau)^2}. \tag{10}$$

Отримані значення дозволяють підвищити точність інтегральної оцінки бічних пелюсток АКФ.

Для рівномірно розподіленої д.в.в. X за відомих математичного сподівання $M(X)$ і дисперсії $D(X)$ оцінка нормованої АКФ може бути обчислена за допомогою виразу

$$r_x'(\tau)=\frac{1}{n}\sum_{i=0}^{n-1}\Big[\left(x_{t+i}-M(X)\right)\cdot\left(x_{t+\tau+i}-M(X)\right)\Big]\Big/D(X). \tag{11}$$

Показано, що статистичний критерій відповідності АКФ досліджуваної послідовності АКФ білого шуму полягає в наступному:

$$n\sum_{\tau=1}^{\mathrm{T}}\left(r_x'(\tau)\right)^2 \to \chi^2_{\mathrm{T}} \qquad (12)$$

Удосконалений критерій оцінювання автокореляції часових рядів на основі одночасного аналізу декількох коефіцієнтів автокореляції шляхом його адаптації для рівномірно розподілених д.в.в. надав можливість виконати комплексну кількісну оцінку АКФ для послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел.

Застосування критерію дало змогу виявити статистичні відхилення для деяких генераторів ПВП, які успішно проходять усі автокореляційні тести пакету TestU01.

Запропоновано нові метод і критерій оцінювання якості послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел на основі дослідження розподілу знаків АКФ.

Для цього досліджувана послідовність довжини $L_{посл}$ розбивається на блоки довжини $L_{блок}$, які можуть перекривати один одного або відставати один від одного. Відстань між сусідніми блоками позначимо через τ $\left(\tau \geq 1 - L_{блок}\right)$. Схему розбивки вибірки на блоки представлено на рис. 11. Діагональним штрихуванням зліва направо зверху донизу позначено області перекриття блоків, а зліва направо знизу догори – області між блоками.

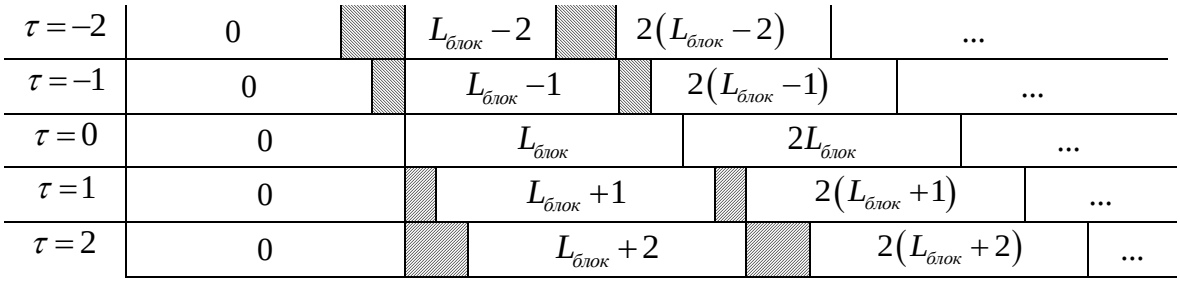


Рис. 11. Схема розбиття вибірки на блоки

Оцінка нормованого коефіцієнта кореляції $r_i(\tau)$ обчислюється для пари блоків із номерами $i\cdot\left(L_{блок}+\tau\right)$ і $(i+1)\cdot\left(L_{блок}+\tau\right)$ наступним чином:

$$r_i(\tau) = \frac{\dfrac{1}{L_{блок}}\displaystyle\sum_{l=0}^{L_{блок}-1}\left(\overset{o}{x}\left(i\cdot\left(L_{блок}+\tau\right)+l\right)\cdot\overset{o}{x}\left(\left(i+1\right)\cdot\left(L_{блок}+\tau\right)+l\right)\right)}{\sqrt{D\left(X\left(i\cdot\left(L_{блок}+\tau\right)\right)\right)}\cdot\sqrt{D\left(X\left(\left(i+1\right)\cdot\left(L_{блок}+\tau\right)\right)\right)}}, \qquad (13)$$

де $\overset{o}{x}(j+l) = x(j+l) - M\left(X(j)\right)$;

$x(j+l)$ – елемент, що знаходиться на позиції $(j+l)$, $0 \leq (j+l) \leq L_{посл}-1$;

$M\left(X(j)\right)$ і $D\left(X(j)\right)$ – математичне сподівання і дисперсія д.в.в. $X(j)$, реалізаціями якої є $L_{блок}$ елементів j-ого блоку.

Обчислюється послідовність знаків $\{z_i(\tau)\} = sign\left(sign\{r_i(\tau)\} + 0.5\right)$. Далі для кожної отриманої послідовності $\{z_i(\tau)\}$ відповідно до критерію χ^2 перевіряється статистична гіпотеза про відповідність розподілу k-грам знаків рівномірному закону, а також перевіряється статистична гіпотеза про відповідність нормальному закону емпіричного розподілу значень функції відносної частоти $W(k,\tau,\alpha)$ потрапляння отриманих значень $\chi_n^2(k,\tau)$ у критичну область. У разі успішної перевірки обчислюються значення бар'єрної функції:

$$\tau_{\min}(k,\alpha,\gamma) = \min\left(-\tau > 0 : W(k,\tau,\alpha) > W_{\max}(\alpha,\gamma)\right), \qquad (14)$$

де $W_{\max}(\alpha,\gamma) = \alpha + t_{(1+\gamma)/2}\sqrt{\alpha(1-\alpha)/N}$.

Застосовується критерій бар'єрної функції: виконується перевірка узгодженості емпіричних розподілів із відносними частотами $\varphi_{k,\gamma}(\alpha) = \tau_{\min}(k,\alpha,\gamma) \Big/ \sum_{\alpha=\alpha_1}^{\alpha_2} \tau_{\min}(k,\alpha,\gamma)$ для $\alpha \in [\alpha_1,\alpha_2]$ з теоретичним граничним (рівномірним) за критерієм χ^2. Тест вважається пройденим, якщо для всіх $k \in [1,K]$ отримані статистики не потрапляють у критичну область критерію χ^2 для заданого рівня значущості β. Розроблено методику застосування критерію.

Результати дослідження джерел рівномірно розподілених випадкових і псевдовипадкових чисел показують, що джерело випадкових чисел, отриманих шляхом оцифрування радіошумів, відповідає розробленому критерію, в той час як реалізація квантового ГВЧ і генератор типу «Вихор Мерсенна» MT19937 не задовольняють вимогам, що пред'являються.

Представлено розроблений критерій оцінювання точності відтворення закону розподілу д.в.в., який базується на твердженні про те, що дискретний випадковий процес, породжений реальним ГВЧ, є композицією двох дискретних випадкових процесів, які відповідно породжують потік символів із теоретичним законом розподілу і потік символів-завад. За цих умов помилка відтворення закону розподілу д.в.в. є числом символів потоку завади, що припадають на одиницю об'єму вибірки. Застосування розробленого критерію до ПВП РЗЛЗЗ і ЛКГ показує, що, наприклад, для забезпечення точності $\xi \le 10^{-3}$: генератор *M*-послідовності повинен мати порядок генераторного полінома $n \ge 10$; ЛКГ, що має структуру графа $O_{M-1} + O_1$, – $M > 1000$. Показано, що перетворення області визначення д.в.в. X шляхом обчислення функції $Y = \lfloor XN_2/N_1 \rfloor$ або $Y = |X|_{N_2}$ призводить до появи конструктивної помилки перетворення. Нульова помилка може бути досягнута шляхом подальшого коригування отриманої послідовності.

Розроблений критерій оцінки точності відтворення закону розподілу д.в.в., а також розглянуті функції перетворення області визначення д.в.в., можуть, наприклад, бути використані під час практичної реалізації методу Фішера-Йєтса формування випадкової послідовності перестановок для приведення випадкового

числа до потрібного діапазону.

У заключному розділі дисертаційної роботи розроблено методологію захисту інформації в телекомунікаційних системах і мережах на основі факторіального кодування даних.

Структурно-аналітичне відображення запропонованої методології захисту інформації на основі факторіального кодування даних наведено на рис. 12.

Розроблена методологія охоплює сім базових етапів.

Етап 1. Формування множини загроз під час передавання інформації каналами зв'язку.

На першому етапі користувачу необхідно визначити можливі загрози, які виникають під час транспортування інформації каналами зв'язку в телекомунікаційних системах і мережах. У результаті реалізації цього етапу формується множина загроз $\mathbf{CT} = \left\{ \bigcup_{i=1}^{N} CT_i \right\} = \{CT_1, CT_2, \ldots, CT_N\}$, де N – кількість можливих загроз, визначених користувачем.

Етап 2. Формування вимог до параметрів кодування та кількісних показників захищеності інформації.

На основі сформованої множини загроз **CT** визначаються множина вимог до параметрів кодування $\mathbf{CR} = \left\{ \bigcup_{i=1}^{N_c} CR_i \right\}$ та множина гранично допустимих кількісних показників захищеності інформації $\mathbf{SR} = \left\{ \bigcup_{i=1}^{N} \bigcup_{j=1}^{L_i} SR_{ij} \right\}$. Для кожної можливої загрози CT_i, $i \in [1, N]$, може формуватися множина показників захищеності $\mathbf{SR}_i = \left\{ \bigcup_{j=1}^{L_i} SR_{ij} \right\} = \{SR_{i1}, SR_{i2}, \ldots, SR_{iL_i}\}$, де L_i – кількість можливих показників для i-ї загрози.

Етап 3. Вибір методу факторіального кодування інформації.

На основі сформованої на першому етапі множині загроз **CT** користувачем обирається метод факторіального кодування інформації. Якщо множина загроз містить загрози $CT_i =$ «*Пошкодження інформації внаслідок помилок каналу*» і $CT_j =$ «*Несанкціонована модифікація інформації криптоаналітиком*», метод факторіального кодування обирається з групи з N_{sep} роздільних методів $\mathbf{FC}sep = \left\{ \bigcup_{i=1}^{N_{sep}} FCsep_i \right\}$. Якщо множина загроз містить загрози $CT_i =$ «*Пошкодження інформації внаслідок помилок каналу*» і $CT_j =$ «*Несанкціоноване ознайомлення з інформацією*», метод факторіального кодування обирається з групи з N_{insep} нероздільних методів $\mathbf{FC}insep = \left\{ \bigcup_{i=1}^{N_{insep}} FCinsep_i \right\}$.

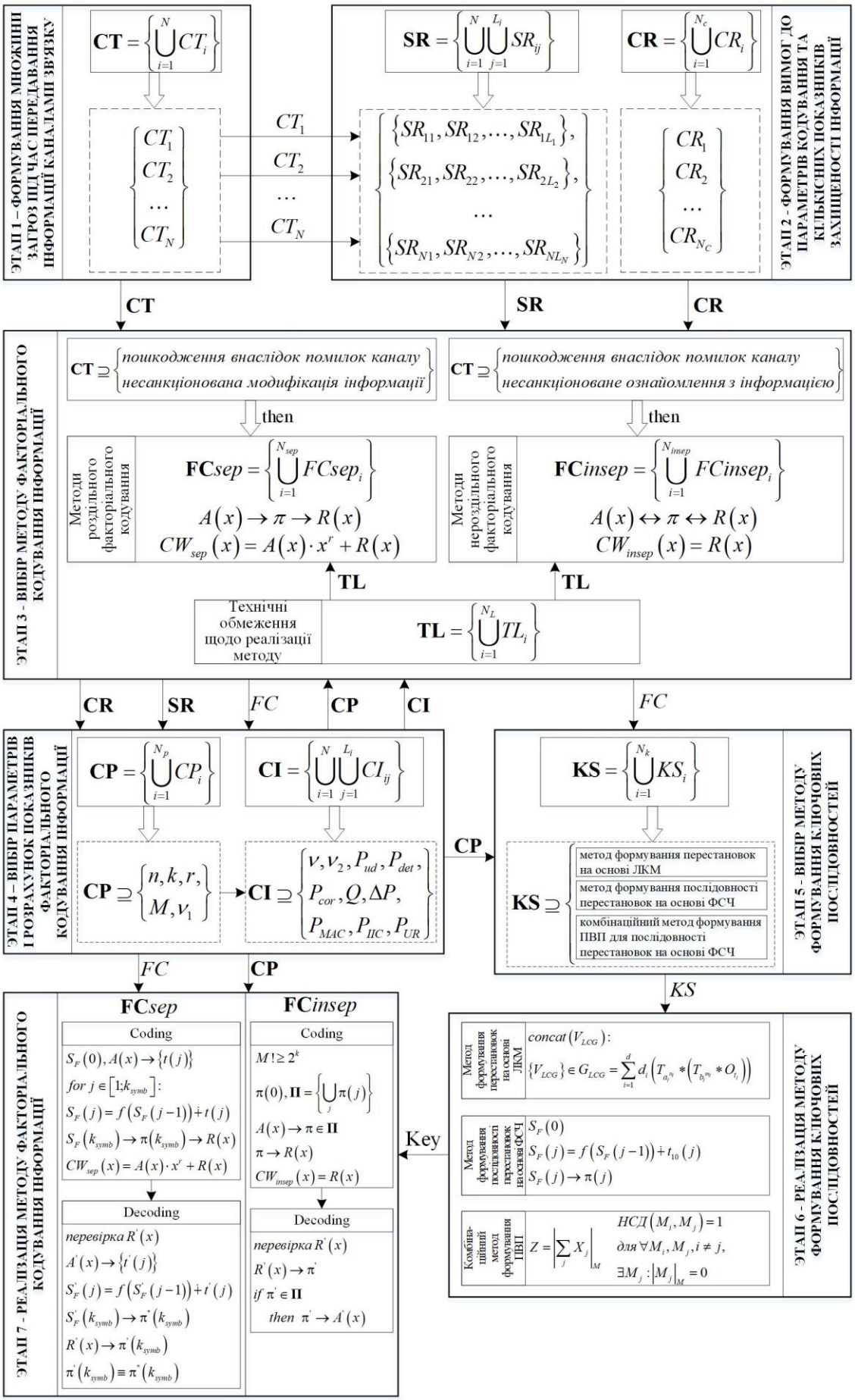


Рис. 12. Структурно-аналітичне відображення методології захисту інформації на основі факторіального кодування даних

Якщо ж множина загроз містить загрози $CT_i =$«*Пошкодження інформації внаслідок помилок каналу*», $CT_j =$«*Несанкціонована модифікація інформації криптоаналітиком*» і $CT_l =$«*Несанкціоноване ознайомлення з інформацією*», користувач може як комбінувати роздільні та нероздільні методи факторіального кодування, так і використовувати метод роздільного факторіального кодування з поєднанням з іншим методом криптографічного закриття інформації, наприклад, методом двоконтурного криптографічного перетворення.

Порядок перестановки M визначається сформованими на другому етапі вимогами.

Вибір методу факторіального кодування базується також на аналізі множини технічних обмежень $\mathbf{TL} = \left\{ \bigcup_{i=1}^{N_L} TL_i \right\} = \left\{ TL_1, TL_2, \ldots, TL_{N_L} \right\}$, а також на порівнянні сформованих на другому етапі методології вимог до параметрів кодування **CR** та кількісних показників **SR** захищеності інформації з параметрами та показниками факторіального кодування, розрахованими на четвертому етапі.

Етап 4. Вибір параметрів і розрахунок показників факторіального кодування інформації.

Для обґрунтованого вибору та реалізації методів факторіального кодування інформації на основі характеристик каналу передавання даних визначаються основні параметри $\mathbf{CP} = \left\{ \bigcup_{i=1}^{N_c} CP_i \right\}$ та кількісні показники $\mathbf{CI} = \left\{ \bigcup_{i=1}^{N} \bigcup_{j=1}^{L_i} CI_{ij} \right\}$ досліджуваного факторіального коду з метою їх задоволення, відповідно, множині **CR** вимог до параметрів кодування та множині вимог **SR** до кількісних показників захищеності інформації.

Етап 5. Вибір методу формування ключових послідовностей.

Для обраного методу факторіального кодування, за визначених на четвертому етапі параметрів коду, обирається метод формування ключових послідовностей з множини з N_K можливих методів $\mathbf{KS} = \left\{ \bigcup_{i=1}^{N_K} KS_i \right\}$. Ця множина включає: $KS_1 =$«метод формування ПВП на основі лінійного конгруентного методу, який дозволяє формувати ПВП рівномірно розподілених чисел незалежно від топології графа станів ЛКГ»; $KS_2 =$«метод формування послідовностей перестановок на основі ФСЧ, який дозволяє уникнути порушення рівномірності розподілу перестановок та підвищити швидкість їх формування»; $KS_3 =$«комбінаційний метод формування ПВП з комбінаційною функцією підсумовування за модулем слів, отриманих від групи первинних генераторів рівномірно розподілених випадкових чисел як із необмеженими, так і з обмеженими періодами, а також перестановок, які циклічно повторюються».

Крім вибору самого методу формування ключової послідовності, в залежності від визначеної на четвертому етапі множини **CP** обираються параметри для його реалізації.

Етап 6. Реалізація методу формування ключових послідовностей для факторіального кодування інформації.

Цей етап передбачає реалізацію обраного на попередньому етапі методу формування ключових послідовностей з визначеними параметрами.

Етап 7. Реалізація методу факторіального кодування інформації.

Сьомий етап передбачає реалізацію обраного на етапі 3 методу факторіального кодування інформації на основі визначених параметрів (етап 4), а також вибору методу формування ключових послідовностей (етап 5) і його реалізації (етап 6).

Розроблена методологія за рахунок формалізованого механізму використання принципів, 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 захисту інформації, що реалізують сумісний захист інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-технічну проблему, яка полягає в створенні методології захисту інформації на основі факторіального кодування даних із необхідними ансамблевими, статистичними, структурними властивостями кодових послідовностей для побудови систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу із забезпеченням підвищення достовірності передавання інформації за однакових обсягів введеної надлишковості.

Найбільш значущі результати роботи полягають у наступному.

1. Удосконалено метод формування випадкової послідовності перестановок порядку M, який унаслідок виключення необхідності приведення випадкового числа до потрібного діапазону зі змінною верхньою межею дозволив уникнути порушення рівномірності розподілу перестановок та зменшити обсяг пам'яті додаткового ГПВЧ не менш ніж на $\log_2 M$ біт. Вивільнений ресурс може бути направлений на реалізацію додаткових сервісних функцій, наприклад, таких, як контроль і діагностика. Реалізація алгоритму формування послідовності перестановок дозволила підвищити швидкість роботи генератора порівняно з генератором перестановок із застосуванням алгоритму Фішера-Йєтса для $M = 5$ – у 2,1 рази; $M = 10$ – у 2,6 рази; $M = 20$ – у 2,8 рази.

2. Розроблено методи роздільного факторіального кодування інформації (ПФК, КФК, ФКП, ФКДКСр), які за рахунок використання множини змінних констант в якості ключа дозволяють забезпечити захист інформації від модифікації внаслідок випадкових і умисних деструктивних дій, забезпечити властивість самосинхронізації коду та підвищити достовірність інформації в умовах обмежень пропускної здатності каналів зв'язку.

3. Розроблено методи нероздільного факторіального кодування інформації (ФКВД, ФКВДд, ФКЗЧІ, ФКДКСн, ФКВДвп), які дозволяють забезпечити її захист від несанкціонованого читання та помилок каналу зв'язку, забезпечити властивість

самосинхронізації коду та підвищити достовірність інформації в умовах обмежень пропускної здатності каналів зв'язку.

4. Розроблено математичну модель процесу декодування факторіальних кодів, яка дозволяє оцінити достовірність передавання інформації в результаті застосування факторіального кодування. Показано, що в порівнянні з використанням циклічного надлишкового коду за однакових обсягів введеної надлишковості для ймовірності помилки в каналі зв'язку $p_0 = 10^{-3}$ ПФК дозволяє досягти енергетичного виграшу до 2,7 дБ для довжини інформаційної частини $k = 1024$ біти та довжини перевірної частини $r = 64$ біти, КФК – до 1,6 дБ для $k = 1024$ біти та $r = 16$ біт, ФКВД – до 0,821 дБ, ФКЗЧІ – до 3,295 дБ (для порядку перестановки 8).

5. Розроблено модель узагальненого графа станів ЛКГ, яка дозволяє виконати класифікацію типів компонент зв'язності графа станів ЛКГ та дослідити вплив параметрів на його топологію. Розроблена модель надала можливість удосконалити метод формування ПВП на основі лінійного конгруентного методу, який дозволяє формувати ПВП рівномірно розподілених чисел незалежно від топології графа станів ЛКГ та, як наслідок, мінімізувати часові витрати на вибір параметрів ЛКГ та збільшити розмір простору їх допустимих значень для досягнення періоду ПВП $T = M$ у $M/\varphi(M)$ разів. Реалізація алгоритму формування псевдовипадкової послідовності перестановок на основі ЛКГ з будь-яким типом графа його станів дозволила підвищити швидкість роботи генератора порівняно з генератором перестановок на основі ГПВЧ LFIB78 із застосуванням алгоритму Фішера-Йєтса для порядку перестановки $M \le 125$: зокрема, для $M = 20$ – у 2,1 рази; $M = 50$ – у 1,6 рази; $M = 100$ – у 1,2 рази.

6. Удосконалено метод симетричного криптографічного захисту інформації, який дозволяє блокувати можливість винесення гами та зменшити ймовірність зламу шифру методом повного перебору ключового простору в $2^{4n} \cdot (n!)^2$ разів, де n – розрядність блоку даних. Розроблено структурну схему та алгоритм роботи пристрою двоконтурного криптографічного перетворення даних, що забезпечують можливість його практичної реалізації. Реалізація алгоритму в режимі формування ПВП дозволяє отримати послідовність, яка успішно проходить тести NIST STS, Diehard, TestU01.

7. Теоретично обґрунтовано принципи побудови комбінаційного генератора, який використовує підсумовування за модулем M в якості комбінаційної функції. Для цього визначено закон розподілу д.в.в. на виході комбінаційного генератора, що містить n первинних генераторів випадкових чисел як із необмеженими, так і з обмеженими періодами, а також перестановок, що циклічно повторюються. Це дало змогу обґрунтувати загальні вимоги до первинних послідовностей і комбінаційної функції для забезпечення рівномірного розподілу чисел у заданому діапазоні, а також розробити методику вибору параметрів первинних генераторів для забезпечення необхідних статистичних властивостей формованої послідовності чисел і її використання в реалізаціях запропонованого методу формування перестановок на основі ФСЧ. Виконана оцінка статистичних властивостей ПВП на виході комбінаційного генератора підтверджує, що запропонований комбінаційний

метод формування ПВП може бути використаний у задачах, що потребують їх високої якості, зокрема, для формування псевдовипадкової послідовності перестановок на основі ФСЧ.

8. Розроблено метод, критерії та методики оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, які дозволяють виявити статистичні властивості, притаманні послідовностям, породженим природними джерелами випадкових чисел, і не притаманні штучно згенерованим ПВП. Застосування розробленого інструментарію дало змогу виявити статистичні відхилення для деяких генераторів ПВП, які успішно проходять усі автокореляційні тести пакету TestU01, а також для реалізації квантового ГВЧ.

9. Розроблено методологію захисту інформації на основі факторіального кодування даних, яка дозволяє забезпечити підтримку процесів створення систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу. Застосування цієї методології дає можливість використовувати розроблені методи та моделі в єдиній стратегії досліджень у галузі інтегрованого захисту інформації в телекомунікаційних системах і мережах та ефективно будувати відповідні системи захисту з заданими властивостями.

10. Результати дисертаційної роботи впроваджено на ДП «НДІ «Акорд», у ТОВ «Діджитал Мастер», у Департаменті освіти та гуманітарної політики Черкаської міської ради та в освітньому процесі Черкаського державного технологічного університету, Черкаського інституту пожежної безпеки імені Героїв Чорнобиля та Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

ОСНОВНІ ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

[1] Э. В. Фауре, "Факториальное кодирование с исправлением ошибок. Теоретическое обоснование и примеры реализации", в *Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: монография*, под ред. В. М. Безрук, и В. В. Баранник, Харьков: Лидер, 2017, с. 291-323.

[2] Е. В. Фауре, "Методологія захисту інформації на основі факторіального кодування даних", в *Криптографічне кодування: обробка та захист інформації: колективна монографія*, під ред. В. М. Рудницький, Харків: Щедра садиба плюс, 2018, с. 85-95.

[3] Э. В. Фауре, В. В. Швыдкий, и В. А. Щерба, "Комбинированное факториальное кодирование и его свойства", *Радіоелектроніка, інформатика, управління*, № 3, с. 80-86, 2016.

[4] E. V. Faure, A. I. Shcherba, and V. M. Rudnytskyi, "The Method and Criterion for Quality Assessment of Random Number Sequences", *Cybernetics and Systems Analysis*, vol. 52, no. 2, pp. 277-284, 2016.

[5] Е. В. Фауре, "Факториальное кодирование с исправлением ошибок", *Радіоелектроніка, інформатика, управління*, № 3, с. 130-138, 2017.

[6] E. V. Faure, A. I. Shcherba, and A. A. Kharin, "Factorial code with a given number of

inversions", *Radio Electronics, Computer Science, Control*, no. 2, pp. 143-153, 2018.
[7] N. Alishov, E. Faure, D. Faure, and V. Shadkhin, "Method of linear formation of pseudorandom processes", *Journal of Qafqaz University. Mathematics and computer science*, no. 30, pp. 17-24, 2010.
[8] Р. О. Бивзюк, Д. В. Фауре, и Э. В. Фауре, "Устройство формирования остатков в многоканальных помехоустойчивых кодеках", *Вісник Хмельницького національного університету*, № 4, с. 75-78, 2010.
[9] Є. В. Ланських, Е. В. Фауре, і А. В. Очеретяна, "Метод організації ключового обміну з використанням прихованого каналу в телефонних мережах загального користування", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 18-21, 2010.
[10] Е. С. Лисицына, В. В. Швыдкий, А. И. Щерба, и Э. В. Фауре, "Разделение векторной смеси сигнала и помехи по методу максимального правдоподобия", *Системи обробки інформації*, № 8(89), с. 62-67, 2010.
[11] Э. В. Фауре, Д. В. Фауре, и И. Н. Коротеев, "Выбор параметров генератора конгруэнтных чисел", *Сучасна спеціальна техніка*, № 1(20), с. 30-35, 2010.
[12] Э. В. Фауре, Д. В. Фауре, М. В. Сторчак, и В. А. Кучеренко, "Исследование и оптимизация методов формирования контрольной суммы помехоустойчивых кодов", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 63-67, 2011.
[13] Р. М. Дідковський, Е. В. Фауре, і В. В. Олексієнко, "Прихована передача інформації у полосі звукових частот", *Сучасний захист інформації*, № 2, с. 22-30, 2011.
[14] Э. В. Фауре, Е. В. Ланских, Д. А. Коляда, и Ю. И. Черевко, "Преобразование процессов на выходе генераторов М-последовательности и конгруэнц-генераторов", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 1, с. 17-21, 2012.
[15] Р. М. Дідковський, Е. В. Фауре, і В. В. Олексієнко, "Ансамбль ортогональних шумоподібних сигналів для скритних систем з обмеженим спектром", *Наукові записки УНДІЗ*, № 1(21), с. 33-38, 2012.
[16] А. С. Береза, А. А. Лавданский, В. В. Швыдкий, и Э. В. Фауре, "Генерация конгруэнтных последовательностей чисел с заданными свойствами", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 2, с. 3-8, 2012.
[17] Э. В. Фауре, А. С. Береза, и Е. А. Ярославская, "Оценка точности воспроизведения закона распределения дискретной случайной величины при ее преобразовании", *Вестник Хмельницкого национального университета*, № 5, с. 176–182, 2012.
[18] В. Ю. Шадхін, Е. В. Фауре, і О. В. Костомаров, "Криптографічні засоби захисту інформації в автоматизованих системах дистанційного навчання", *Вісник Хмельницького національного університету*, № 1, с. 126-130, 2012.
[19] В. В. Швыдкий, Э. В. Фауре, В. В. Веретельник, и В. А. Щерба, "Генерация стохастической последовательности генератором конгруэнтных чисел", *Системи обробки інформації*, № 3, с. 74-80, 2012.
[20] Ю. Г. Лега, Э. В. Фауре, и А. А. Лавданский, "Технология генерации случайных

последовательностей с большой разрядностью чисел", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 3, с. 3-8, 2012.

[21] А.А. Лавданский, В.В. Швыдкий, и Э.В. Фауре, "Метод формирования последовательностей случайных чисел и его использование в системах потокового шифрования", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 1, с. 5-10, 2013.

[22] Э. В. Фауре, Е. С. Лисицына, и Д. Ю. Нестеренко, "Метод повышения стойкости электронных кодовых замков", *Вісник Інженерної академії України*, № 2, с. 137-141, 2013.

[23] Е. В. Фауре, М. І. Вишня, і В. А. Чорнобай, "Оцінка закону розподілу випадкових чисел комбінаційного генератора у k-вимірному просторі", *Вісник Херсонського національного технічного університету*, № 4(51), с. 169-173, 2014.

[24] Э. В. Фауре, В. В. Швыдкий, и А. И. Щерба, "Метод формирования воспроизводимой непредсказуемой последовательности перестановок", *Безпека інформації*, т. 20, № 3, с. 253-258, 2014.

[25] Э. В. Фауре, "Закон распределения дискретной случайной величины на выходе комбинационного генератора", *Безпека інформації*, т. 20, № 2, с. 153-158, 2014.

[26] А. А. Лавданский и Э. В. Фауре, "Оценка статистических свойств последовательностей на выходе комбинационного генератора с помощью графических тестов", *Системні дослідження та інформаційні технології*, № 2, с. 39-50, 2015.

[27] Е. В. Фауре, С. В. Сисоєнко, і Т. В. Миронюк, "Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення", *Системи управління, навігації та зв'язку*, № 4(36), с. 85-87, 2015.

[28] Э. В. Фауре, В. В. Швыдкий, и В. А. Щерба, "Метод формирования имитовставки на основе перестановок", *Захист інформації*, т. 16, № 4, с. 340, 2015.

[29] Э. В. Фауре, А. И. Щерба, и А. А. Лавданский, "Анализ корреляционных свойств последовательностей (псевдо) случайных чисел", *Наука і техніка Повітряних Сил Збройних Сил України*, № 1(18), с. 142-150, 2015.

[30] Э. В. Фауре, А. И. Щерба, и А. А. Лавданский, "Оценка статистических характеристик последовательности псевдослучайных чисел, порожденной комбинационным генератором", *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*, № 18, с. 165-171, 2015.

[31] В. М. Рудницький, Е. В. Фауре, і С. В. Сисоєнко, "Оцінка якості псевдовипадкових послідовностей на основі додавання за модулем", *Вісник Інженерної академії України*, № 3, с. 219-221, 2016.

[32] Э. В. Фауре, "Факториальное кодирование с восстановлением данных", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 2, с. 33-39, 2016.

[33] Э. В. Фауре, "Метод повышения эффективности факториального кодирования с восстановлением данных", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 57-61, 2016.

[34] Э. В. Фауре, "Факториальное кодирование с несколькими контрольными

суммами", *Вісник Житомирського державного технологічного університету. Серія: Технічні науки*, № 3 (78), с. 104-113, 2016.

[35] Э. В. Фауре, В. В. Швыдкий, и А. И. Щерба, "Контроль целостности информации на основе факториальной системы счисления", *Journal of Baku Engineering University. Mathematics and computer science*, т. 1, № 1, с. 3-13, 2017.

[36] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий, і А. І. Щерба, "Спосіб комбінованого кодування інформації", патент України №107657, 24.06.2016.

[37] Е. В. Фауре, Д. В. Фауре, і Р. О. Бівзюк, "Пристрій формування залишків у багатоканальних завадостійких кодеках", патент України №55711, 27.12.2010.

[38] В. В. Швидкий, А. І. Щерба, Е. В. Фауре, і В. В. Веретельник, "Спосіб формування некорельованої послідовності рівномірно розподілених чисел", патент України №74628, 12.11.2012.

[39] Ю. Г. Лега, В. В. Швидкий, Е. В. Фауре, А. І. Щерба, і А. О. Лавданський, "Спосіб двоконтурного поточного шифрування", патент України №82044, 25.07.2013.

[40] Е. В. Фауре, В. В. Швидкий, і А. І. Щерба, "Спосіб формування випадкової послідовності перестановок", патент України №106668, 10.05.2016.

[41] Е. В. Фауре, В. В. Швидкий, і А. І. Щерба, "Спосіб формування імітовставки", патент України №106669, 10.05.2016.

[42] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий, і А. І. Щерба, "Спосіб контролю цілісності інформації", патент України №107655, 24.06.2016.

[43] А. О. Лавданський, Е. В. Фауре, В. В. Швидкий, і А. І. Щерба, "Спосіб формування послідовності рівномірно розподілених випадкових чисел", патент України №86718, 10.01.2014.

[44] Ю. Г. Лега, В. В. Швидкий, Е. В. Фауре, О. С. Лісіцина, і А. О. Лавданський, "Спосіб формування послідовності випадкових чисел", патент України №86705, 10.01.2014.

[45] Е. В. Фауре, О. О. Харін, В. В. Швидкий, і А. І. Щерба, "Спосіб факторіального кодування з відновленням даних", патент України №117004, 12.06.2017.

[46] Е. В. Фауре, О. О. Харін, В. В. Швидкий, і А. І. Щерба, "Спосіб факторіального кодування з виявленням і виправленням помилок", патент України №121361, 11.12.2017.

[47] Е. В. Фауре і О. О. Харін, "Пристрій кодування та декодування факторіальних кодів з виявленням і виправленням помилок", патент України №123640, 12.03.2018.

[48] Э. В. Фауре и А. А. Лавданский, "Способ определения структуры графа состояний линейного конгруэнтного генератора", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 18-22 березня 2013 р.*, Черкаси, 2013, с. 110-112.

[49] E. Faure, V. Chornobai, and M. Vyshnia, "Some statistical properties of pseudorandom number sequences formed by combination generator", in *Современные достижения в науке и образовании : сб. тр. IX междунар. науч. конф., 22-29 сентября 2014 г., Нетания (Израиль).*, Хмельницкий, 2014, pp. 56-58.

[50] А. А. Лавданский и Э. В. Фауре, "Комбинационный метод формирования последовательности псевдослучайных чисел", в *Системний аналіз та інформаційні технології: матеріали 16-ї Міжнародної науково-технічної конференції SAIT-2014, Київ, 26-30 травня 2014 р.*, К., 2014, с. 403-404.

[51] Э. В. Фауре и В. В. Швыдкий, "Формирование имитовставки на основе перестановок", в *Проблеми інформатизації: Матеріали другої міжнародної науково-технічної конференції, Черкаси, 25-26 листопада 2014 р.*, Черкаси, 2014, с. 12.

[52] Е. В. Фауре і А. М. Ткаченко, "Дослідження здатності виявлення помилок завадостійким кодом на основі перестановок", в *Проблеми інформатизації: Матеріали третьої міжнародної науково-технічної конференції, Черкаси, 12-13 листопада 2015 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2015, с. 17.

[53] Э. В. Фауре, "Статистические характеристики оценок нормированных коэффициентов автокорреляции последовательностей (псевдо) случайных чисел", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 16-20 березня 2015 р.*, Черкаси, 2015, с. 46-47.

[54] Э. В. Фауре и А. В. Магуров, "Исследование способности обнаружения ошибок комбинированным факториальным кодом", в *Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4 листопада 2016 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 13.

[55] Е. В. Фауре і С. В. Сисоєнко, "Метод підвищення стійкості псевдовипадкових послідовностей до лінійного криптоаналізу", в *The scientific potential of the present [text]: Proceedings of the International Scientific Conference, St. Andrews, Scotland, UK, December 1, 2016*, Vinnytsia, 2016, с. 119-122.

[56] Э. В. Фауре и Р. К. Еременко, "Исследование способности обнаружения ошибок полным факториальным кодом", в *Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4 листопада 2016 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 12.

[57] Е. В. Фауре і О. О. Харін, "Дослідження ймовірності виникнення помилки декодування під час використання факторіального коду з відновленням даних", в *Актуальні задачі та досягнення у галузі кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції, Кропивницький, 23-25 листопада 2016 р.*, Кропивницький, 2016, с. 178-179.

[58] Э. В. Фауре, "Методика оценки вероятности преобразования перестановки чисел в перестановку при ее передаче по каналу связи", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 14-20 березня 2016 р.*, Черкаси, 2016, с. 78-80.

[59] Е. В. Фауре, О. О. Харін, і М. О. Качалова, "Дослідження процедури

формування контрольної суми повного факторіального коду на основі ітераційного перетворення", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 17.

[60] Е. В. Фауре і В. С. Рузальонок, "Дослідження структури графа станів лінійного конгруентного генератора", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 15-16.

АНОТАЦІЯ

Фауре Е.В. Методологія захисту інформації на основі факторіального кодування даних. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Національний авіаційний університет, Київ, 2018.

Дисертаційна робота спрямована на вирішення актуальної науково-технічної проблеми створення методології захисту інформації на основі факторіального кодування даних з необхідними ансамблевими, статистичними, структурними властивостями кодових послідовностей для побудови систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу.

У роботі вдосконалено метод формування випадкової послідовності перестановок, який дозволив уникнути порушення рівномірності їх розподілу, зменшити розрядність додаткового ГПВЧ та підвищити швидкість роботи генератора. Розроблено методи роздільного факторіального кодування інформації, які дозволяють забезпечити її захист від модифікації внаслідок випадкових і умисних деструктивних дій, забезпечити властивість самосинхронізації та підвищити показники достовірності в умовах обмежень пропускної здатності каналів зв'язку. Розроблено методи нероздільного факторіального кодування інформації, які дозволяють забезпечити її захист від несанкціонованого читання та помилок каналу зв'язку, забезпечити властивість самосинхронізації та підвищити показники достовірності в умовах обмежень пропускної здатності каналів зв'язку. Розроблено математичну модель процесу декодування факторіальних кодів, яка дозволяє оцінити їх показники достовірності. Розроблено модель узагальненого графа станів лінійного конгруентного генератора, яка дозволяє виконати класифікацію типів компонент зв'язності графа і дослідити вплив параметрів на його топологію. Удосконалено метод формування ПВП на основі лінійного конгруентного методу, який дозволяє формувати ПВП рівномірно розподілених чисел незалежно від топології графа станів генератора, мінімізувати часові витрати на вибір параметрів ЛКГ та збільшити розмір простору їх допустимих значень для досягнення максимального періоду. Удосконалено метод симетричного криптографічного захисту інформації, який дозволяє виключити можливість

винесення гами та підвищити стійкість до статистичного криптоаналізу. Теоретично обґрунтовано принципи побудови комбінаційного генератора на основі підсумовування за модулем, що дозволило сформулювати загальні вимоги до параметрів генератора. Розроблено метод, критерії та методики оцінювання послідовностей випадкових чисел. Розроблено методологію захисту інформації на основі факторіального кодування даних, яка дає можливість використовувати розроблені методи та моделі в єдиній стратегії досліджень в галузі інтегрованого захисту інформації в телекомунікаційних системах і мережах та ефективно будувати відповідні системи захисту з заданими властивостями.

Ключові слова: захист інформації, конфіденційність, цілісність, достовірність, факторіальне кодування, псевдовипадкова послідовність, генератор випадкових чисел, оцінювання випадкових послідовностей.

АННОТАЦИЯ

Фауре Э.В. Методология защиты информации на основе факториального кодирования данных. – На правах рукописи.

Диссертация на соискание научной степени доктора технических наук по специальности 05.13.21 – Системы защиты информации. – Национальный авиационный университет, Киев, 2018.

Диссертация направлена на решение актуальной научно-технической проблемы создания методологии защиты информации на основе факториального кодирования данных с необходимыми ансамблевыми, статистическими, структурными свойствами кодовых последовательностей для построения систем защиты информации от ошибок канала связи, несанкционированной модификации и/или несанкционированного доступа.

В работе усовершенствован метод формирования случайной последовательности перестановок, который позволил избежать нарушения равномерности их распределения, уменьшить разрядность дополнительного генератора псевдослучайных чисел и повысить скорость работы генератора. Разработаны методы разделимого факториального кодирования информации, которые позволяют обеспечить ее защиту от модификаций вследствие случайных и умышленных деструктивных воздействий, обеспечить свойство самосинхронизации и повысить показатели достоверности в условиях ограничений пропускной способности каналов связи. Разработаны методы неразделимого факториального кодирования информации, которые позволяют обеспечить ее защиту от несанкционированного чтения и ошибок канала связи, обеспечить свойство самосинхронизации и повысить показатели достоверности в условиях ограничений пропускной способности каналов связи. Разработана математическая модель процесса декодирования факториальных кодов, которая позволяет оценить их показатели достоверности. Разработана модель обобщенного графа состояний линейного конгруэнтного генератора, которая позволяет выполнить классификацию типов компонент связности графа и исследовать влияние параметров на его топологию. Усовершенствован метод формирования псевдослучайных последовательностей (ПСП) на основе линейного конгруэнтного метода, позволяющего формировать ПСП равномерно распределенных чисел независимо от

топологии графа состояний генератора, минимизировать временные затраты на выбор параметров линейного конгруэнтного генератора и увеличить размер пространства их допустимых значений для достижения максимального периода. Усовершенствован метод симметричной криптографической защиты информации, который позволяет исключить возможность выноса гаммы и повысить устойчивость к статистическому криптоанализу. Теоретически обоснованы принципы построения комбинационного генератора на основе суммирования по модулю, что позволило сформулировать общие требования к параметрам генератора. Разработан метод, критерии и методики оценки последовательностей случайных чисел. Разработана методология защиты информации на основе факториального кодирования данных, которая дает возможность использовать разработанные методы и модели в единой стратегии исследований в области интегрированной защиты информации в телекоммуникационных системах и сетях и эффективно строить соответствующие системы защиты с заданными свойствами.

Ключевые слова: защита информации, конфиденциальность, целостность, достоверность, факториальное кодирование, псевдослучайная последовательность, генератор случайных чисел, оценивание случайных последовательностей.

ABSTRACT

Faure E. Methodology of information security based on factorial data coding. – Manuscript.

Thesis for a Doctor of Technical Science degree in specialty 05.13.21 – Information security systems. – National Aviation University, Kyiv, 2018.

The thesis is devoted to the actual scientific and technical problem of creating the methodology of information security in telecommunication systems and networks based on factorial data coding with necessary ensemble, statistical, and structural properties of code sequences for building systems of information security against communication channels errors, unauthorized modifications and/or unauthorized access.

It is shown that to date, the developed methods of integrating channel coding and encryption exist only for broadband telecommunication systems. However, these methods do not allow controlling data integrity. The solution of the problem of providing a complex information security provides related problems associated with the improvement of existing and development of new methods of cryptographic transformation and methods of generating and estimating sequences of random and pseudorandom numbers.

It is improved the method of generating unpredictable sequence of permutations of order M that allows to avoid the problem of disruption of permutations uniform distribution due to the elimination of need to transform a random number to a range with variable upper limit, and reduce capacity of additional pseudorandom number generator at least by $\log_2 M$ bit. The implementation of the algorithm of permutation sequence formation allowed to increase the generator speed, compared with the Fisher–Yates shuffle for $M = 5$ – by 2.1 times; $M = 10$ – by 2.6 times; $M = 20$ – by 2.8 times.

The methods of separable factorial coding of information are developed. These methods, by using a set of variable constants as a key, can provide complex information security from modifications due to accidental and intentional destructive actions, provide

the property of code self-synchronization, and improve the measures of reliability in conditions of bandwidth restrictions.

The methods of inseparable factorial coding of information are developed. These methods allow providing complex information security against unauthorized reading and channel errors, providing the property of code self-synchronization, and increasing the reliability of information in conditions of bandwidth restrictions.

The mathematical model of decoding of factorial codes is developed. The model allows evaluating the reliability of information transmission with factorial coding. It is shown that compared to CRC for the same amount of input redundancy and bit error rate $p_0 = 10^{-3}$ full factorial code achieves energy gain to 2.7 dB for the length of information part $k = 1024$ bits and the length of check part $r = 64$ bits, combined factorial code – up to 1.6 dB with $k = 1024$ bits and $r = 16$ bits, factorial code with data recovery by permutation – up to 0.821 dB, factorial code with a given number of inversions – up to 3.295 dB (for permutation order 8).

The model of generalized states graph of linear congruential generator is developed. It allows to perform classification of connected components of its graph and to investigate the impact of parameters on its topology. The model allowed to improve the method of pseudo-random sequences (PRS) forming based on linear congruential method, which allows to form uniformly distributed PRS of numbers independently from generator graph topology, minimize the time for choosing its parameters, increase by $M/\varphi(M)$ times the size of space of their permissible values. Also it allowed increasing the generator speed (compared with the generator based on LFIB78 PRNG using Fisher–Yates shuffle for $M \le 125$: for $M = 20$ – by 2.1 times; $M = 50$ – by 1.6 times; $M = 100$ – by 1.2 times).

The method of symmetric cryptographic data protection is improved. It allows excluding the possibility of gamma disclosure and increasing the resistance to statistical cryptanalysis. It is theoretically grounded the principles of construction of combination generator with summation modulo as a combining function. It made possible to prove general requirements for primary sequences and combining function to ensure uniform distribution of numbers in a given range.

The method, criteria and techniques of estimating of uniformly distributed random and pseudo-random sequences that can detect statistical properties inherent to sequences generated by natural sources of random numbers and no inherent to artificially generated PRS. Implementation of the developed methods and criteria allowed identifying statistical deviations for some PRS generators, which successfully pass all autocorrelation tests of TestU01 package, as well as for one implementation of quantum RNG.

The methodology of information security based on factorial data coding has been developed. It allows supporting the processes of creation of information security systems that implement the joint data protection from communication channel errors, unauthorized modifications and/or unauthorized access. Application of the methodology makes it possible to use the developed methods and models in a united research strategy in the field of integrated information security in telecommunication systems and networks and to effectively build appropriate security systems with given properties.

Key words: information security, confidentiality, integrity, reliability, factorial coding, pseudorandom sequence, random number generator, random sequence estimation.