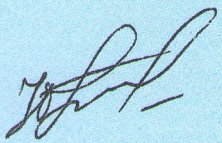
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності

**БОРЗОВ ЮРІЙ ОЛЕКСІЙОВИЧ**



УДК 004.832.3:519.711.2

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПІДВИЩЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ КРИТИЧНОГО ЗАСТОСУВАННЯ

05.13.06 – інформаційні технології

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Львів – 2015

**Дисертацією є рукопис.**
Роботу виконано у Львівському державному університеті безпеки життєдіяльності Державної служби України з надзвичайних ситуацій

**Науковий керівник:** доктор технічних наук, доцент
**Рак Тарас Євгенович,**
Львівський державний університет безпеки життєдіяльності, проректор з науково-дослідної роботи

**Офіційні опоненти:** доктор технічних наук, професор
**Андрощук Олександр Степанович,**
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, начальник докторантури – головний науковий співробітник

доктор технічних наук, професор
**Теслюк Василь Миколайович,**
Національний університет "Львівська політехніка", професор кафедри систем автоматизованого проектування

Захист відбудеться " 10 " грудня 2015 р. о 14.00 годині на засіданні спеціалізованої вченої ради К 35.874.02 Львівського державного університету безпеки життєдіяльності (79007, м. Львів, вул. Клепарівська, 35)

З дисертацією можна ознайомитись у науковій бібліотеці Львівського державного університету безпеки життєдіяльності (79007, м. Львів, вул. Клепарівська, 35)

Автореферат розісланий " 10 " листопада 2015 р.

Учений секретар
спеціалізованої вченої ради О. Б. Зачко

# ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність роботи**. Технологічний розвиток суспільства призвів до постійно зростаючого впровадження інформаційних технологій у найрізноманітніші області людської діяльності. У результаті новий поштовх отримала автоматизація управління функціонуванням та бізнес-діяльністю суб'єктів господарювання на основі впровадження інформаційних та інформаційно-управляючих систем. Одним із актуальних напрямів впровадження технологій таких систем є автоматизація діяльності об'єктів підвищеної небезпеки та потенційно небезпечних об'єктів, які, зазвичай функціонують в online режимах чи режимах реального часу. Системи такої автоматизації отримали назву інформаційних або інформаційно-управляючих систем критичного застосування і до них, типово, відносять автоматизовані системи раннього виявлення надзвичайних ситуацій та оповіщення (АСРВО), медичні системи, системи Smart House, системи управління складними та небезпечними виробництвами і об'єктами, аварії на яких можуть привести до масштабних надзвичайних ситуацій тощо.

Визначальною характеристикою цих систем є те, що їх функціонування має значний вплив на ефективність забезпечення життєдіяльності людей. Це зумовлено тим, що процеси прийняття рішень щодо управління системами критичного застосування (локалізації, ліквідації надзвичайних ситуацій тощо.) включають передачу комунікаційними системами та аналіз персоналом або автоматизованими системами відеоінформації, спотворення якої може призвести до помилкових рішень.

До якісних атрибутів окремих видів систем критичного застосування, а це в першу чергу стосується систем управління безпекою соціальних об'єктів та систем управління безпекою, відносять функціональну безпеку, яка визначає у широкому розумінні функціонування системи у відповідності до визначених наперед вимог. Під безпекою систем розуміють таке їх функціонування, при якому відсутні небезпечні відмови та недопустимі втрати. Причинами відмов можуть бути дефекти програм, даних, апаратури, впливи зовнішнього середовища.

Для забезпечення необхідного рівня функціональної безпеки при вирішення проблем передачі інформації в реальних системах критичного застосування необхідне комплексне використання різних методів. До таких методів можна віднести: завадостійке кодування, стиснення відеоінформації, криптографічне перетворення тощо. Завадостійке кодування виконується з метою захисту від випадкових завад та допомагає ефективно використовувати комунікаційні канали для надійної передачі інформації. Стиснення використовується для зменшення обсягу переданої інформації. Під стисненням розуміють кодування даних з метою представлення інформації в більш компактному вигляді.

Основною архітектурною особливістю окремих видів систем критичного застосування є їх розподіленість, а відтак існування комунікаційних ка-

налів. При цьому важливою складовою інформаційних пакетів в комунікаційних сеансах дуже часто використовуються цифрові зображення різних типів. Відповідно, гарантування стійкого, надійного і захищеного передавання зображень комунікаційними каналами є елементом забезпечення безпеки обробки інформації в інформаційно-управляючих системах критичного застосування мережевої архітектури. У результаті підвищується рівень загальної функціональної безпеки та забезпечується живучість і збільшується ефективність функціонування інформаційно-управляючих систем критичного застосування.

Підвищенням рівня функціональної безпеки в системах, заснованих на комунікаційних сеансах, є використання інформаційних технологій на основі криптографічного кодування. Такі засоби вважаються найбільш ефективними на сьогодні.

Тобто основними категоріями забезпечення функціональної безпеки СППР (система прийняття правильних рішень) на підставі відео зображень виступають стійкість, надійність та безпечність процесів технічної обробки та управління інформацією, що циркулює в автоматизованій системі. Стійкість та надійність забезпечуються методами стійкого та надійного кодування. А безпека – різноманітними криптографічними перетвореннями тощо.

Проблеми розробки інформаційних технологій підвищення надійності та безпеки даних, зокрема в комунікаційних сеансах, відображено в працях К. Шеннона, М. Діффі, М. Хеллмана, В. К. Задіраки, І. Д. Горбенка, В. Я. Чечельницького, М. П. Карпінського, Ю. М. Коростіля, О. А. Курченка. Серед існуючої великої кількості криптографічних перетворень особливе місце займає асиметрична система криптографічного кодування RSA. При великих значеннях ключів кодування та декодуванняця криптосистема визначає високий рівень безпеки, що призвело до того, що алгоритм практичної реалізації криптосистеми став промисловим стандартом і визначає напрями розвитку інформаційних технологій забезпечення функціональної безпеки.

У випадку використання криптографічного кодування на основі стандарту RSA для цифрових зображень виникає проблема, яка полягає у тому, що на закодованому зображенні можуть зберігатись контури (флуктуації функції інтенсивності). У цьому випадку атака на об’єкт захисту може полягати не у зламі самого алгоритму, а у використанні методів цифрової обробки зображень (фільтрації, реконструкції) для отриманні основної інформативності цього зображення.

Отримані на сьогодні результати теоретичних та практичних досліджень надають можливість уникнути появи контурів на зашифрованих зображеннях при достатньо малих значеннях ключів. Проте, вони характеризується або високою обчислювальною складністю, або значними інформаційними втратами, які виникають в процесах забезпечення функціональної безпеки. Їх практичне використання є витратним з точки зору мінімізації ресурсів для забезпечення високого рівня функціональної безпеки.

Функціональна безпека систем, що розглядаються забезпечується низкою засобів, кожен з яких використовує певні часові, обчислювальні

ресурси тощо. Науково-методичні підходи застосування універсальних засобів, що поєднують у собі декілька функцій на даний час є не достатньо розвинутими.

Тому *актуальною науковою задачею* є розробка інформаційної технології забезпечення функціональної безпеки інформаційно-управляючих систем критичного застосування, які базуються на комунікаційних процедурах із застосуванням універсальних засобів з метою мінімізації обчислювальних ресурсів в процесах забезпечення надійності, стійкості та безпеки функціонування цих систем.

**Зв'язок роботи з науковими програмами, планами, темами.**

Тематика дисертаційної роботи, її мета і основні завдання відповідають державній програмі забезпечення пожежної безпеки в Україні на 2012-2015 рр., державним науково-технічним програмам, сформульованим в Законі України "Про науково-технічну діяльність" та в Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки". Робота виконувалася у рамках науково-дослідних робіт "Створення навчального макету автоматизованої системи оперативно-диспетчерського управління для підготовки та перепідготовки диспетчерів та керівного складу ОДС" (0114U004183), "Розроблення методичних рекомендацій з організації служби оперативного зв'язку, телекомунікаційних систем та інформаційних технологій в системі ДСНС України" (0114U004185), "Розробка методів і моделей захисту інформаційно-комунікаційних систем і мереж у структурних підрозділах ДСНС України" (0114U004275).

**Мета і задачі дослідження.** Метою дисертаційної роботи є розроблення інформаційних технологій для забезпечення необхідного рівня функціональної безпеки інформаційно-управляючих систем критичного застосування та зменшенні витрат при передаванні зображень в комунікаційних сеансах.

Для досягнення поставленої мети в роботі необхідно розв'язати такі часткові задачі:

1) провести аналіз ефективності методів та засобів забезпечення функціональної безпеки при передаванні зображень комунікаційними каналами інформаційно-управляючих систем критичного застосування;

2) розробити метод забезпечення функціональної безпеки систем критичного застосування для випадку використання повноколірних зображень завдяки сумісному використання криптосистем Ель-Гамаля і RSA;

3) удосконалити метод забезпечення необхідного рівня функціональної безпеки систем критичного застосування у випадку циркуляції в телекомунікаційних сеансах напівтонових зображень із глибиною кольору в 1-2 байти, який ґрунтується на інтегральному поєднанні елементів алгоритму криптографічного кодування RSA та операції зашумлення;

4) розробити метод забезпечення функціональної безпеки, який базується на використанню бінарних операцій в інтегральному поєднанні із елементами алгоритму RSA для побудови стійких алгоритмів забезпечення функціональної безпеки інформаційно-управляючих систем критичного застосування;

5) розробити інформаційну технологію підвищення функціональної безпеки для мережевих інформаційно-управляючих систем критичного застосування та програмно її реалізувати для забезпечення різних складових функціональної безпеки;

6) провести аналіз ефективності використання розроблених методів та інформаційної технології забезпечення функціональної безпеки у інформаційно-управляючих системах з комунікаційними каналами.

**Об'єктом дослідження** є процес обробки інформації для забезпечення функціональної безпеки в системах підтримки прийняття рішень в комунікайних сеансах інформаційно-управляючих систем критичного застосування на підставі цифрових зображень.

**Предметом дослідження** є методи, засоби та інформаційні технології підвищення функціональної безпеки комунікаційних сеансів при передаванні зображень.

**Методи дослідження.** Результати дисертаційних досліджень отримані з використанням елементів інформаційних технологій, теорії інформаційних систем, цифрової обробки зображень, теорії безпеки інформації, теорії чисел, лінійної та булевої алгебр, дискретної математики, топології, математичного аналізу та комп'ютерного моделювання.

**Наукова новизна отриманих результатів**. На основі виконаних теоретичних та експериментальних досліджень отримано такі результати:

*вперше розроблено*:

- метод забезпечення необхідного рівня функціональної безпеки систем критичного застосування, який ґрунтується на сумісному використанні систем криптографічного кодування Ель-Гамаля і RSA, що дає можливість підвищити стійкість функціонування інформаційних систем при передаванні в комунікаційних процедурах цифрових зображень із глибиною кольору до 4 байт із зменшенням витрат;

*отримав подальший розвиток:*

- метод забезпечення необхідного рівня функціональної безпеки систем критичного застосування у випадку циркуляції в телекомунікаційних сеансах напівтонових зображень із глибиною кольору в 1-2 байти, який ґрунтується на інтегральному поєднанні елементів алгоритму криптографічного кодування RSA та операції зашумлення, що дало можливість збільшити рівень безпеки систем без інформаційних втрат;
- метод забезпечення функціональної безпеки на основі алгоритму RSA, який завдяки використанню бінарних операторів забезпечує необхідне значення стійкості та унеможливлює несанкціоноване відтворення методами цифрової оброки сигналів повноколірних зображень із глибиною кольору у 3-4 байти в комунікаційних процесах систем критичного застосування;

*удосконалено:*

- інформаційну технологію забезпечення необхідного рівня функціональної безпеки для випадку передавання комунікаційними каналами

напівтонових зображень із глибиною кольору в 1-2 байти, яка базується на використанні модифікованого методу RSA та порозрядних операцій, що дає можливість усунути контури на зображеннях та зменшує витрати обчислювальних ресурсів в програмній реалізації процедур забезпечення функціональної безпеки.

**Практичне значення одержаних результатів**. Отримані результати досліджень є основою розробленої програмної бібліотеки, яка призначена для забезпечення функціональної безпеки при передаванні зображень у комп'ютерних мережах на основі протоколів TCP, UDP та Http.

Усі розроблені методи на відміну від існуючих підходів характеризуються достатньою стійкістю і надійністю у порівнянні із криптографічним кодуванням RSA і дають змогу створювати інформаційні технології, які не вимагають для свого функціонування значних обчислювальних ресурсів.

Усунення контурів в розроблених методах здійснюється при малих значеннях ключів процедур криптографічного кодування, що гарантує невихід за межі розрядної сітки в обчислювальному процесі.

Підвищення функціональної безпеки у випадку передавання комунікаційними каналами напівтонових зображень із глибиною кольору в 1-2 байти забезпечується удосконаленою інформаційною технологією з високим значенням стійкості, яке рівна: $4 \cdot 16^4 \cdot (\varphi(\psi(n)) - 1) \cdot \Omega(n)$(тут $\varphi$ – функція Ейлера, а $\psi$ – найменше спільне кратне чисел ($P$– 1) і ($Q$– 1,які, у свою чергу, визначають відкриту і закриту частину ключа, та число $n = PQ$, $\Omega(n)$– стійкість криптографічного кодування).

Сумісне використання елементів криптографічних кодувань RSA та Ель-Гамаля дозволило отримати метод забезпечення функціональної безпеки, який володіє стійкістюу $(P - 3)^2$ разів більшою у порівнянні із базовим аглоритмом.

Програмно побудовано динамічну бібліотеку, яка реалізовує технологію захисту зображень. Особливістю цієї бібліотеки є можливість її використання як для персоніфікованої функціональної безпеки, так і для забезпечення функціональної безпеки у комунікаційних сеансах автоматизованих систем.

Результати дисертаційних досліджень також використовувались в Головному управлінні ДСНС у Львівській області при розробці та впровадженні системи оперативно-диспетчерського управління (СОДУ) та Системи 112 (акт про використання результатів досліджень від 24 червня 2014 року).

Результати роботи використовуються у навчальному процесі Львівського державного університету безпеки життєдіяльності на кафедрі управління інформаційною безпекою при викладанні дисципліни «Безпека інформації в інформаційно-комунікаційних системах» тема «Протоколи передавання та захисту інформації, захист комп'ютерних мереж»(акт про використання результатів досліджень від 11 лютого 2015 року).

**Особистий внесок здобувача**. Основні положення та результати дисертаційної роботи автор отримав самостійно. У друкованих працях, опублікованих у співтоваристві, авторові належать: схема використання порозряд-

них операцій в модифікаціях алгоритму RSA за одним та двома рядками [4, 8, 12], метод використання бінарних операцій при криптографічному кодуванні кольорових зображень [2], реалізація оператора зашумлення в шифруванні напівтонових [6, 9, 11] та кольорових зображень [5], сумісне використання побітових операцій та оператора зашумлення при захисті кольорових зображень [7, 10], алгоритм сумісного використання криптосистем RSA Ель-Гамаля при криптографічному кодуванні за одним та двома рядками [1, 3].

**Апробація результатів дисертації**. Результати дисертаційної роботи доповідалися на таких науково-технічних конференціях:

- The VI$^{th}$ International Scientific and Technical Conference [“Computer Science and Information Technologies” (CSIT 2011)], (Lviv, November 16-19, 2011);
- Міжнародна наукова конференція [«Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту»], (Херсон, 16-20 травня 2011);
- Міжнародна наукова конференція [«Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту»], (Херсон, 27-31 травня 2012).

**Публікації.** Матеріали дисертації опубліковано в 12 наукових працях, з них: 8 – у фахових виданнях України з технічних наук (з них 6 входять до міжнародних наукометричних баз), 1 – у закордонному виданні, яке індексується міжнародними наукометричними базами та 3 – у матеріалах міжнародних науково-технічних конференцій.

**Структура і обсяг роботи**. Дисертація складається зі вступу, 4 розділів, висновків та додатків. Загальний обсяг роботи – 141 сторінок, з них основний текст – 107 сторінок. Робота містить 54 рисунків на 37 сторінках та 2 додатки на 17 сторінках. Список використаних літературних джерел складається із 144 найменування і викладений на 17 сторінках.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

***У вступі*** обґрунтовано актуальність дисертаційної роботи, сформульовано мету та задачі наукового дослідження, наукову новизну і практичне значення, подано відомості про особистий внесок автора, апробацію та структуру роботи.

***У першому розділі*** проаналізовано якісні атрибути сучасних систем критичного застосування, виділено характеристики сучасних підходів організації функціональної безпеки в автоматизованих системах критичного застосування, розглянуто принципи побудови засобів функціональної безпеки та проаналізовано проблеми забезпечення стійкості при використанні зображень в телекомунікаційних сеансах методом RSA.

Встановлено чотири базові підходи наукових досліджень у напрямі модифікацій алгоритму RSA для підвищення функціональної безпеки в автоматизованих системах критичного застосування.

Перший підхід полягає у розвитку симетричних методів і його основним недоліком є інформативні втрати, що є критичним у випадку функціонування автоматизованих систем на засадах інтелектуального аналізу даних.

Другий підхід полягає у послідовному використанні алгоритму RSA і оператора зашумленння. Однак такий дво-процедурний підхід не може вважатись криптографічним методом. Більше того, ізоморфні оператори зашумлення легко виявляються шумовими детекторами і усуваються спеціалізованими фільтрами. А використання неізоморфних операторів призводить, подібно до першого підходу, до інформаційних втрат.

Третій підхід називається топологічним і полягає у попередній топологічній обробці самого зображення. Недоліком цього підходу є породження додаткової інформації, а саме інформації про саму топологію і необхідність її передавання комунікаційними каналами. А це, у свою чергу, збільшує робоче навантаження у комунікаційних каналах.

Четвертий підхід полягає у інтеграції оператора зашумлення у саму систему криптографічного кодування RSA. Така інтеграція посилює стохастику зашумлення і унеможливлює детекцію і усунення зашумлення спеціалізованими засобами. Проте більшість модифікацій алгоритму RSA, базованих на використанні інтегрованого оператора зашумлення, недоліком мають зростання розміру зашифрованих даних у порівнянні з вихідними. У випадку цифрових зображень цей недолік посилюється зазвичай великими кількостями вхідних даних.

Основні дослідження і найбільші результати в задачах підвищення функціональної безпеки отримані у модифікації криптосистеми RSA, яка визначає збільшення зашумленості на закодованому зображенні, зосереджено у поєднанні елементів алгоритму RSA та різноманітних алгебраїчних афінних форм. Завдяки такому сумісному використанню отримано такі модифікації алгоритму RSA, які дають можливість уникнути появи контурів на закодованому зображеннях при невеликих значеннях ключів і характеризуються, у порівнянні із самим методом RSA, підвищеною стійкістю.

Недоліком сумісного використання алгебраїчних афінних форм і елементів алгоритму RSA є висока обчислювальна складність, що призводить до зростання обчислювальних ресурсів, особливо у системах реального часу чи on-line системах.

Результати аналізу наукових досліджень показують, що найефективнішим напрямом вирішення проблеми підвищення функціональної стійкості автоматизованих систем критичного застосування є розроблення інформаційних технологій на основі інтегрального поєднання елементів алгоритму RSA і операторів зашумлення при створенні стійких методів інформаційного захисту зображень в автоматизованих системах критичного застосування.

***У другому розділі*** запропоновано підвищення функціональної безпеки для випадку передавання в комунікаційних сеансах напівтонових зображень, які базуються на використанні елементів алгоритму RSA, побітових операцій, бінарних операторів та функцій зашумлення.

Найпростішим із розроблених методів функціональної безпеки є модифікація методу RSA, яка базується на додатковому використанні побітових операцій.

Кодування за одним рядком матриці цифрового зображення в алгоритмічній формі можна подати так:

1. Випадково вибирається натуральне просте число $e < \varphi(N)$ ($e$ взаємно просте з $\varphi(N)$) і знаходиться таке натуральне $d$, що виконується конгруенція

$$ed \equiv 1(\mathrm{mod}\varphi(N)). \tag{1}$$

2. Будується число

$$A = (e<<k) + (d<<l) + (e<<l) + (d<<k), \tag{2}$$

де $k < 16$ , $l < 16$ – натуральні числа, $k \neq l$, << – операція логічного зсуву вліво.

3. У кожному рядку виконується логічний зсув вліво значення інтенсивності $i$-го пікселя, $i = 1, 2, \ldots, m$, $m$ – число елементів у рядку, за наступним правилом:

$$c_{i,j} = c_{i,j} << \begin{cases} i(\mathrm{mod}\,3), \text{ якщо } i(\mathrm{mod}17) \equiv 0; \\ i(\mathrm{mod}\,4), \text{ якщо } i(\mathrm{mod}11) \equiv 1. \end{cases} \tag{3}$$

4. Будується число $B$ відніманням від отриманого значення інтенсивності пікселя числа $(A - 3)$.

5. Кодоване значення інтенсивності $i$-го пікселя визначається так

$$C \equiv B^e(\mathrm{mod}N). \tag{4}$$

Декодування проводиться в порядку, протилежному до кодуванню після отримання числа

$$C^d \equiv (B^e)^d(\mathrm{mod}N), \tag{5}$$

виконанням протилежних операції до змісту пунктів 4-1.

Кодування за двома рядками здійснюється з використанням двох рядків за описаним вище алгоритмом 1-5. При цьому п. 5 має вигляд:

Для першого рядка закодованим значенням інтенсивності $i$-го пікселя, $i = 1, 2, \ldots, m$, $m$ – число елементів у рядку, вибирається число $C \equiv B^e(\mathrm{mod}N)$.

Для другого рядка закодованим значенням інтенсивності $i$-го пікселя вибирається число

$$C \equiv B^d(\mathrm{mod}N). \tag{6}$$

Декодування відбувається в протилежному порядку з урахуванням п.1, 2.

Функціональна стійкість розробленої модифікації алгоритму RSA за методикою Вербіцького О.В. дорівнює: $4 \cdot 16^4 \cdot (\varphi(\psi(n)) - 1)$.

Для оцінки рівнів втрат та зростання рівня зашумленості використовувались метрики попіксельного порівняння, PSNR та різниця значень ентропії.

За цими метриками результати практичних експериментів засвідчили відсутність інформаційних втрат, зростання рівня зашумленості та відсутність контурів при середніх значень ключів.

Розвитком наведеного методу є додаткове внесення зашумленості в процедуру кодування. Алгоритмічно кодування за одним рядком матриці напівтонового зображення можна представити так:

1. За (1) і (2) випадково вибирається натуральне число $e$ <φ($N$) і знаходяться натуральне $d$ та число $A$.

2. У кожному рядку виконується логічний зсув вліво значення інтенсивності $i$-го піксела ($i$ = 1, 2, …, $m$, $m$ – число елементів у рядку) за наступним правилом: виконується логічний зсув вліво значення інтенсивності пікселя на величину $i(\mathrm{mod}n)$, $n$ < 16.

$$c_{i,j} = c_{i,j} << i\left(\mathrm{mod}\, n\right),\ \ n<16\,. \tag{7}$$

3. Будується число $B$ відніманням від отриманого значення інтенсивності пікселя числа ($A$ + $e$).

4. Закодованим значенням інтенсивності $i$-го пікселя вибирається число

$$C\equiv B^e(\mathrm{mod}N) + f(i^2). \tag{8}$$

де $f(i^2)$ – квадратичний оператор зашумлення.

Декодування проводиться в порядку, протилежному до кодування після отримання числа

$$(C - f(i^2))^d \equiv (B^e)^d(\mathrm{mod}N), \tag{9}$$

виконанням протилежних операції до змісту пунктів 4-1.

Кодування за двома рядками відбувається з використанням елементів двох рядків за алгоритмом, який описано вище, за виключенням п. 4, який тепер має вигляд:

Для першого рядка закодованим значенням інтенсивності $i$-го піксела, $i$ = 1, 2, …, $m$, $m$ – число елементів у рядку, вибирається число

$$C\equiv B^e(\mathrm{mod}\ N) + g(i^2). \tag{10}$$

де $g(i^2)$ – оператор зашумлення на випадок кодування за двома рядками.

Для другого рядка закодованим значенням інтенсивності $i$-го пікселя, $i$ = 1, 2, … , $m$, $m$ – число елементів у рядку, вибирається число

$$C\equiv B^e\ (\mathrm{mod}N) - g(i^2). \tag{11}$$

Декодування відбувається в протилежному порядку з урахуванням (10) та (11).

Оцінка результатів практичного застосування здійснювалась подібно до попереднього методу.

На рис. 1, 2 наведено результати кодування напівтонового однобайтового зображення розміром 667 × 332 пікселів при такій парі простих чисел $P$ = 79, $Q$ = 89. З наведених зображень можна побачити повну відсутність контурів. Окрім цього, використання функції зашумлення забезпечує гармонізацію закодованого зображення, що може бути використаним як додатковий елемент захисту. Інформаційні втрати при декодуванні також відсутні.

Рисунок 1 – Початкове зображення

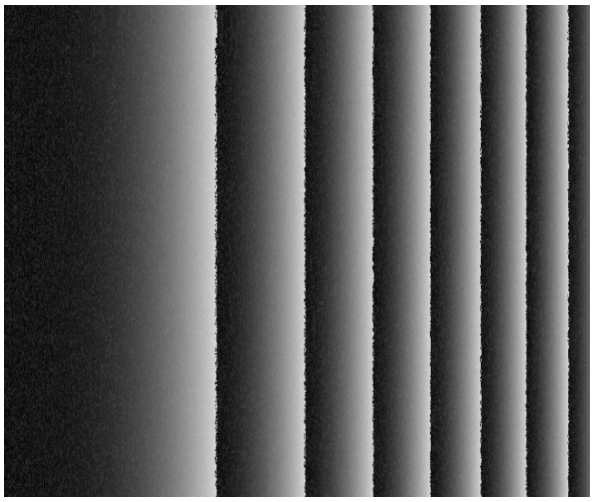


Рисунок 2 – Закодоване зображення

Для підвищення стійкості пропонується метод з поелементним кодуванням та оператором зашумленості, алгоритмічне представлення якого є таким:

1. Випадково вибирається натуральне число $e$ <φ($N$) ($e$ взаємо просте з φ($N$)) і знаходиться таке натуральне $d$, що виконується конгруенція (1).

2. Будуються чотири числа

$$\begin{aligned} &A \equiv \left(c_{k,i}\right)^e \left(\mathrm{mod}\, N\right), B \equiv \left(c_{k+1,i}\right)^e \left(\mathrm{mod}\, N\right), \\ &E \equiv \left(c_{k,i+1} + i^2 / (ed)\right)^d \left(\mathrm{mod}\, N\right), \\ &D \equiv \left(c_{k+1,i+1} + k^2 / (ed)\right)^d \left(\mathrm{mod}\, N\right),\ 1 \le k < n, 1 \le i < m. \end{aligned} \tag{12}$$

3. Будується матриця закодованих значень інтенсивностей пікселів, елементи якої визначаються так

$$\begin{aligned} &b_{k,i} = A + f(k,i), \quad b_{k+1,i} = B + g(k,i), \\ &b_{k,i+1} = E + F(k,i), b_{k+1,i+1} = D + G(k,i),\ 1 \le k < n, 1 \le i < m. \end{aligned} \tag{13}$$

4. Декодування проводиться наступним чином. Декодовані значення інтенсивностей пікселів отримуються з наступних співвідношень:

$$
\begin{aligned}
c_{k,i} &\equiv \left( \text{ж}_{k,i} - f\left(k,i\right)\right)^d \left(\mathrm{mod}\, N\right),\\
c_{k+1,i} &\equiv \left( \text{ж}_{k+1,i} - g\left(k,i\right)\right)^d \left(\mathrm{mod}\, N\right),\\
c_{k,i+1} &\equiv \left( \text{ж}_{k,i+1} - F\left(k,i\right)\right)^e \left(\mathrm{mod}\, N\right) - i^2 / \left(ed\right), \qquad (14)\\
c_{k+1,i+1} &\equiv \left( \text{ж}_{k+1,i+1} - G\left(k,i\right)\right)^e \left(\mathrm{mod}\, N\right) - k^2 / \left(ed\right),\\
f\left(k,i\right) &= Pk^2i^2, g\left(k,i\right) = Qk^2i^2, F\left(k,i\right) = ek^2i^2, G\left(k,i\right) = dk^2i^2.
\end{aligned}
$$

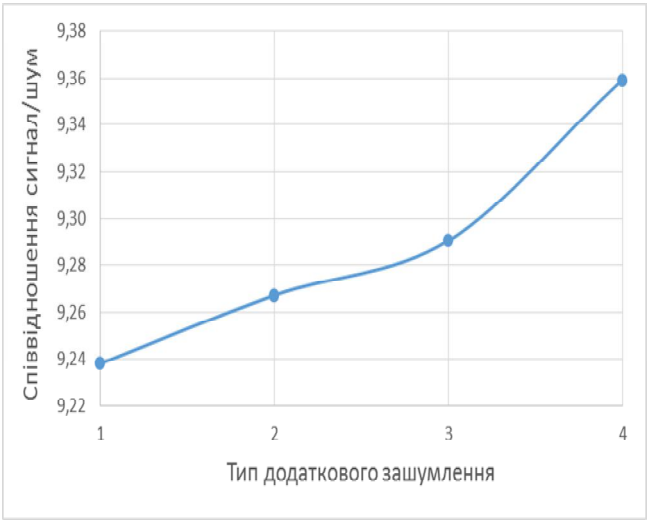
Декодування відбувається в протилежному порядку з урахуванням п.1,2.

Стійкість до декодування розробленого методу становить: $((n - 1) \cdot (m - 1))^4 \cdot (\varphi(\psi(n)) - 1)$.

Практичні експерименти проводились на однотоновому зображенні, розміром 640 х 386 пікселів, з використанням операторів зашумленості, перелік яких наведеного на рис. 3а, та значеннях простих чисел: $P$ = 43, $Q$ = 67. На рис. 4 наведено результати кодування, з яких можна спостерігати ефект структуризації закодованого зображення. Цей ефект поглиблюється із зростанням степенів поліноміальних операторів зашумлення. Треба також відзначити, що це зростання має вплив на збільшення значення PSNR, яке наведено на рис. 3б.

| Позначення | Вид |
|---|---|
| #1 | $f(k,i)=Pk^2i^2, g(k,i)=Qk^2i^2,$ $F(k,i)=ek^2i^2, G(k,i)=Pk^2i^2$ |
| #2 | $f(k,i)=Pk^3i^2, g(k,i)=Qk^3i^2,$ $F(k,i)=ek^2i^2, G(k,i)=Pk^2i^2$ |
| #3 | $f(k,i)=Pk^3i^2, g(k,i)=Qk^3i^2,$ $F(k,i)=ek^3i^2, G(k,i)=Pk^3i^2$ |
| #4 | $f(k,i)=Pk^3i^4, g(k,i)=Qk^3i^4,$ $F(k,i)=ek^3i^4, G(k,i)=Pk^3i^4$ |

а)




б)

Рисунок 3 – Оператори зашумлення (а) та зміна значення *PSNR* між оригінальним та закодованими зображеннями в залежності від використання цих операторів (б)

***У третьому розділі*** запропоновано методи підвищення функціональної безпеки для випадку передавання комунікаційними каналами повноколірних зображень, які базуються на використанні криптосистем RSA та Ель-Гамаля, порозрядних операцій, бінарних операторів та операторів зашумлення.

Перший метод полягає у використання порозрядних та бінарних операцій над елементами матриці інтенсивностей.

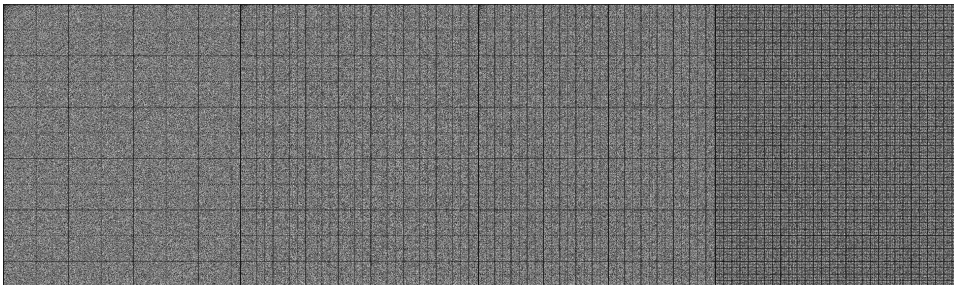



Рисунок 4 – Вплив функції зашумлення на результат кодування

У випадку кодування за одним рядком матриці інтенсивності алгоритмічне представлення має вигляд:

1. Випадково вибирається натуральне число $e < \varphi(N)$ ($e$ взаємно просте з $\varphi(N)$) і знаходиться таке натуральне $d$, що виконується конгруенція (1).

2. Якщо $i \equiv 0 \pmod 2$, $1 \le i \le l$, то випадково вибирається число $m \equiv (i + P) \pmod{31}+1$,і будуються числа $B \equiv m^e \pmod N$, $X = i \cdot B \cdot P$.

3. Якщо $i \equiv 1 \pmod 2$, $1 \le i \le l$, то випадково вибирається число $m \equiv (i + Q) \pmod{31}+1$, і будуються числа $B \equiv m^d \pmod N$, $X = i \cdot B \cdot Q$.

4. З використанням бінарної операції «XOR» будується число $a_{i,j} = c_{i,j} \wedge X$.

5. Виокремлюється кожний розряд $a_{\varpi,i,j}$ числа $a_{i,j}$ за наступною схемою:

$$a_{\varpi,i,j} = a_{i,j} \,\&\, 2^{\varpi-1}; \varpi = \overline{1,32}\,. \qquad (15)$$

де & – операція логічного «І».

6. Виконується циклічне заміщення $m + 1$ розрядів числа $a$ за схемою:

$$a_{\varpi,i,j} = a_{\varpi,i,j} << m+1; \varpi = \overline{1,32}\,. \qquad (16)$$

7. Формуються числа $u_{i,j} = a_{1,i,j} | \ldots | a_{32,i,j}$, які записуються у матрицю $\mathbf{V} = < u_{i,j} >_{i=1..h}^{l=1..l}$.

Декодування у цьому випадку проводиться при заданих числах $e < \varphi(N)$ і $d$, $N$, визначених за (1) і (2), наступним чином:

1. Якщо $i \equiv 0 \pmod 2$, $1 \le i \le l$, то будується число $m \equiv B^d \pmod N$ і число $X = i \cdot B \cdot P$.

2. Якщо $i \equiv 1 \pmod 2$, $1 \le i \le l$, то будується число $m \equiv B^e \pmod N$ і число $X = i \cdot B \cdot Q$.

3. Виокремлюється кожний розряд $a_{\varpi,i,j}$ числа $a_{i,j}$ за схемою (15).

4. Виконується циклічне заміщення $m + 1$ розрядів числа $a$ за схемою (16).

5. З використанням бінарної операції «XOR» будується число

$$c_{i,j} = a \wedge X. \tag{17}$$

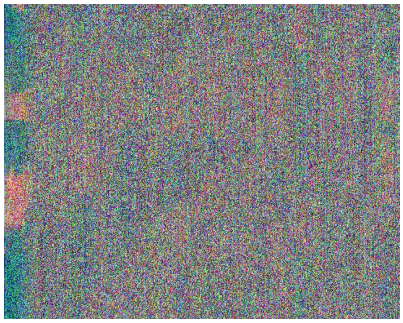
Декодованим є зображення після 5-го кроку.

На рис. 5 наведено результати практичного використання алгоритму кодування на основі описаного методу. Використовувалось повноколірне зображення (колірна система ARGB) розміром 640x386 пікселів. З наведених результатів можна побачити повну зашумленість закодованого зображення при достатньо малих значеннях ключів. Очевидно, що із зростанням значень ключів зростає рівень зашумленості, про що свідчить зростання метрики RSNR, наведене на рис. 6.

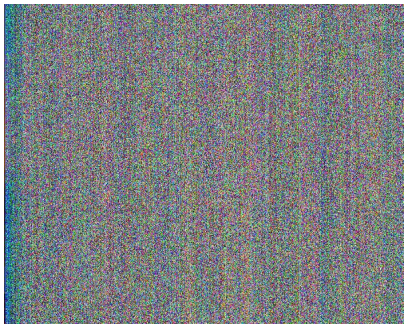
У роботі для сумісного використання порозрядних та побітових операцій наведено також схема використання двох рядків матриці зображення.

Використання бінарних операторів при криптографічному кодуванні повноколірних зображень можна посилити, ввівши в процедуру матрицю ключів. При заданій парі P і Q кодування відбувається поелементно для кожного рядка і алгоритмічно відображається так:

а) початкове зображення для кодування



б) закодоване зображення при значеннях: $P = 71$, $Q = 83$



в) закодоване зображення при значеннях: $P = 127$, $Q = 53$

Рисунок 5 – Результати кодування повноколірних зображень з використанням елементів алгоритму RSA, порозрядних та бінарних операцій

1. Якщо виконується конгруенція: $j(\mathrm{mod}\ 2) \equiv 0$, то будується число:

$$\begin{aligned} jj &= \mathrm{random}(j + P)(\mathrm{mod}\, 31) + 1, \\ a_{i,j} &\equiv jj^{e}(\mathrm{mod}\, N), \quad X = ja_{i,j}P. \end{aligned} \tag{18}$$

2. Якщо виконується конгруенція: $j(\mathrm{mod}\ 2) \equiv 1$, то будується число:

$$\begin{aligned} jj &= \mathrm{random}(j + Q)(\mathrm{mod}\, 31) + 1, \\ a_{i,j} &\equiv jj^{d}(\mathrm{mod}\, N), \quad X = ja_{i,j}Q. \end{aligned} \tag{19}$$

3. Надалі будується число $K = c_{i,j} \wedge X$.

4. Кодоване з $c_{i,j}$ значення $\mathfrak{C}_{i,j}$ отримується циклічним зсувом числа $K$ на $(31 - jj)$ розрядів.

5. Результатом роботи є матриця кодованих значень інтенсивностей пікселів вхідної матриці і матриця ключів.


Рисунок 6 – Залежність метрики *PSNR* від значень *P* і *Q* при використанні методу порозрядних та бінарних операцій в процедурі кодування повноколірного зображення

Декодування проводиться при заданих числах $e < \varphi(N)$ і $d$, $N$, наступним чином:

1. Якщо виконується конгруенція: $j(\mathrm{mod}\ 2) \equiv 0$, то будується число:

$$\begin{aligned} jj &= \mathrm{random}(j + P)(\mathrm{mod}\, 31) + 1, \\ a_{i,j} &\equiv jj^{d}\,(\mathrm{mod}\, N), \quad X = ja_{i,j}P. \end{aligned} \tag{20}$$

2. Якщо виконується конгруенція: $j(\mathrm{mod}\ 2) \equiv 1$, то будується число:

$$\begin{aligned} jj &= \mathrm{random}(j + Q)(\mathrm{mod}\, 31) + 1, \\ a_{i,j} &\equiv jj^{e}\,(\mathrm{mod}\, N), \quad X = ja_{i,j}Q. \end{aligned} \tag{21}$$

3. Виконується циклічний зсув закодованого значення функції інтенсивності $\mathfrak{C}_{i,j}$ на $(31 - jj)$ розрядів.

Результатом роботи є матриця кодованих значень інтенсивностей пікселів, яка визначається так $\mathbf{C} = \mathfrak{C} \wedge X$ .

Найвищої функціональної стійкості в процесі дисертаційних досліджень вдалось досягти при сумісному використанні криптосистем RSA та Ель-Гамаля. У цьому випадку алгоритмічне представлення процедури кодування за одним рядком є таким:

1. Випадково вибирається натуральне просте число $e<\varphi(N)$ таке, що $e$ і $\varphi(N)$ є взаємно простими і виконується конгруенція (1).

2. Випадково вибирається натуральне число $x$: $1<x<P-1$, і $k$: $1<k<P-1$.

3. Будуються чотири числа

$$a \equiv Q\ ,\ b \equiv \left(Q^x \left(\mathrm{mod}\, P\right)\right)^k,$$
$$a_{i,j} \equiv i\left(i+j\right)^e \left(\mathrm{mod}\, N\right)\ ,\ b_{i,j} \equiv j\left(ij\right)^d \left(\mathrm{mod}\, N\right), \tag{22}$$

4. Будується матриця закодованих значень інтенсивностей пікселів, елементи якої визначаються так

$$\begin{aligned} \text{Ж}_{i,j} &= ac_{i,j} - bc_{i,j+1} + a_{i,j} + f\left(i,j\right); \\ \text{Ж}_{i,j+1} &= ac_{i,j} + bc_{i,j+1} + b_{i,j} + g\left(i,j\right), \end{aligned} \tag{23}$$

де $f(i, j)$, $g(i, j)$ – деякі функції зашумлення, $1 \le i \le n$, $1 \le j < m$.

Декодування відбувається наступним чином:

1. Декодовані значення інтенсивностей пікселів отримуються з співвідношень (27):

$$\begin{aligned} ac_{i,j} - bc_{i,j+1} &= \text{Ж}_{i,j} - a_{i,j} - f\left(i,j\right); \\ ac_{i,j} + bc_{i,j+1} &= \text{Ж}_{i,j+1} - b_{i,j} - g\left(i,j\right). \end{aligned} \tag{24}$$

2. Визначаються декодовані значення функції інтенсивності матриці C

$$\begin{aligned} c_{i,j} &= \frac{\left(a\left(\text{Ж}_{i,j} - a_{i,j} - f\left(i,j\right)\right) + b\left(\text{Ж}_{i,j+1} - b_{i,j} - g\left(i,j\right)\right)\right)}{\delta}; \\ c_{i,j+1} &= \frac{\left(a\left(\text{Ж}_{i,j+1} - b_{i,j} - g\left(i,j\right)\right) - b\left(\text{Ж}_{i,j} - a_{i,j} - f\left(i,j\right)\right)\right)}{\delta}, \end{aligned} \tag{25}$$

де $\delta = a^2 + b^2$.

Стійкість кодування описаного методу визначається співвідношенням: $(P-3)^2 \cdot (\varphi(\psi(n)) - 1)$.

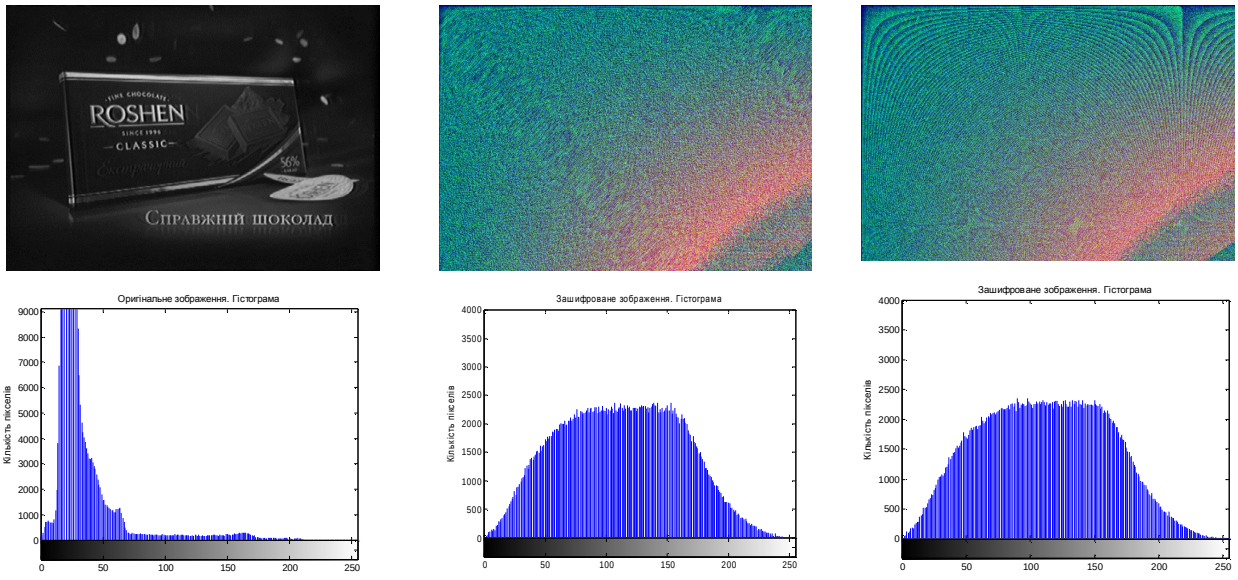
У роботі також наведена схема використання двох рядків за умови сумісного використання алгоритмів RSA та Ель-Гамаля.

На рис.7 наведено приклад практичного використання методу сумісного використання криптосистем RSA та Ель-Гамаля. Параметри процедури кодування були такими: зображення розміру 552x575 пікселів у палітрі ARGB, пара простих чисел: $P = 23$, $Q = 19$.

З наведених на рис.7 результатів видно повну відсутність контурів при дуже малих значеннях простих чисел. Відзначити треба також те, що вплив методу на гістограму має нормалізаційний характер.

***У четвертому розділі*** запропоновано інформаційну технологію підвищення функціональної безпеки для випадку передавання цифрових зображень в телекомунікаційних процедурах та основні архітектури автоматизованих систем критичного застосування стосовно використання цієї технології.

Суть запропонованої інформаційної технології полягає у появі в технологічному процесі “кодування – комунікація – декодування” етапів вибору алгоритму та контролю результатів роботи процедур функціональної безпеки. Перший з них полягає у автоматизованому виборі алгоритму кодування в залежності від типу зображень і обмежень, які накладає обчислювальне середовище. Другий етап полягає у перевірці якості результатів кодування через оцінку контурів на закодованому зображенні.




а) початкове зображення для кодування та його гістограма

б) закодоване за одним рядком зображення та його гістограма

в) закодоване за двома рядками зображення та його гістограма

Рисунок 7 – Результати кодування повноколірних зображень на основі сумісного використанням криптосистем RSA та Ель-Гамаля

Для реалізації розробленої інформаційної технології в автоматизованих системах критичного застосування виокремлено і модифіковано три типові архітектури, зокрема: однорангової системи, системи із виділеним сервером та розподіленої систем. Так на рис. 8 наведено схема реалізації інформаційної технології захисту в розподіленій автоматизованій системі.

У програмній реалізації розроблено бібліотеку засобів підвищення функціональної безпеки зображень та на її основі програмний примітив однорангової мережевої автоматизованої системи, архітектурна схема якого наведена на рис. 9.

Прикладними характеристиками розробленого програмного рішення є мережеві сеанси та захист зображень. Захист реалізовується функціями динамічної бібліотеки crypto. В сукупності із розробленим єдиним

користувацьким інтерфейсом її підключення дає змогу реалізувати технологію Plug-Play для швидкого оновлення функцій кодування та розширення їх набору.

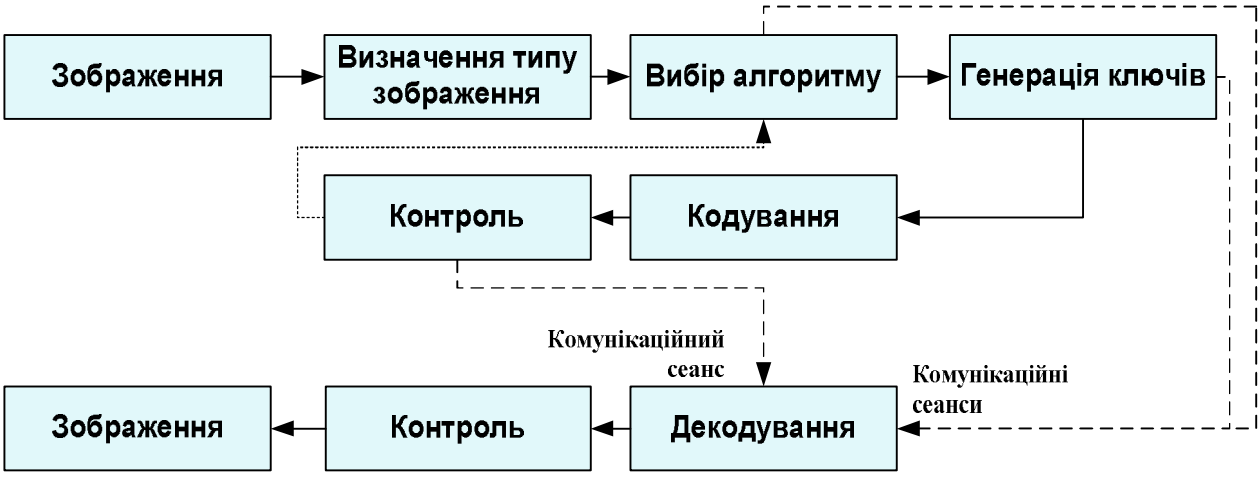



Рисунок 8 – Структура модифікованої інформаційної технології передавання зображень комунікаційними каналами зображень

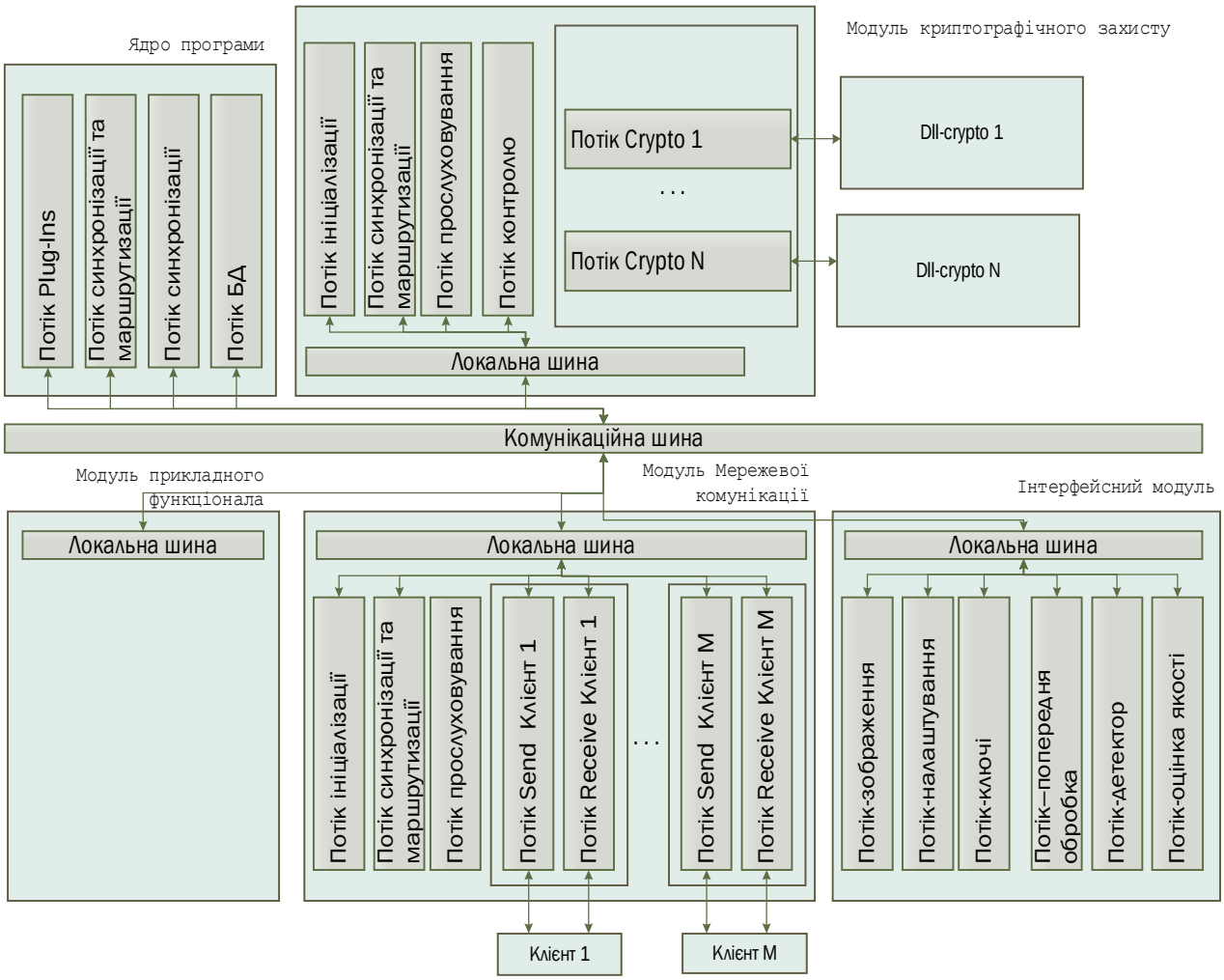



Рисунок 9 – Архітектура програмної реалізації примітиву однорангової автоматизованої системи із підвищеним рівнем функціональної безпеки

Архітектурно програмний примітив – це функціональні паралельні потоки, синхронізація роботи яких здійснюється ядром програми за допомогою спільної комунікаційної шини. Такий підхід підвищує стійкість роботи програми.

Реалізація мережевих сеансів здійснена на основі технології сокетів, що дає можливість відділити прикладний рівень програмного рішення від системного.

Варто відзначити, що бібліотека засобів підвищення функціональної безпеки є окремим програмним рішенням і може використовуватись у будь-якому іншому програмному додатку, наприклад для персоніфікованого захисту зображень та інформації.

# ВИСНОВКИ

У дисертаційній роботі розв’язано актуальну науково-прикладну задачу, яка полягає у розробці інформаційної технології підвищення функціональної безпеки інформаційно-управляючих систем критичного застосування, які базуються на комунікаційних процедурах із застосуванням універсальних засобів з метою мінімізації обчислювальних ресурсів в процесах забезпечення надійності, стійкості та безпеки функціонування цих систем.

При цьому отримано такі науково-практичні результати:

1. На підставі опрацювання літературних джерел проаналізовано відомі інформаційні технології забезпечення функціональної безпеки при передаванні потоків даних у форматі цифрових зображень комунікаційними каналами інформаційно-управляючих систем критичного застосування. Функціональна безпека систем, що розглядаються забезпечується низкою засобів, кожен з яких використовує певні часові, обчислювальні ресурси тощо. Науково-методичні підходи застосування універсальних засобів, що поєднують у собі декілька функцій на даний час є не достатньо розвинутими.

2. Сумісне використання для кодування систем Ель-Гамаля і RSA дозволило отримати метод підвищення функціональної безпеки систем критичного застосування при передаванні в комунікаційних процедурах цифрових зображень із глибиною кольору до 4 байт, що дає можливість підвищити стійкість функціонування інформаційних системв $(P-3)^2 \cdot (\varphi(\psi(n))-1)$.

3. Використання елементів криптографічного кодування RSA та операції зашумлення дало можливість удосконалити метод забезпечення необхідного рівня функціональної безпеки в процедурах захисту напівтонових зображень із глибиною кольору в 1-2 байти, що дало можливість збільшити рівень безпеки систем без інформаційних втрат в комунікаційних процедурах автоматизованих систем критичного застосування.

4. Інтегрування бінарних операторів в схему криптографічного кодування дало можливість підвищити загальний рівень функціональної безпеки систем оброки і комунікаційного обміну повноколірних зображень в автоматизованих системах критичного застосування.

5. Удосконалена інформаційна технологія підвищення функціональної безпеки для випадку передавання комунікаційними каналами напівтонових зображень із глибиною кольору в 1-2 байти завдяки використанню елементів алгоритму RSA та порозрядних операцій, що дає можливість забезпечити повну зашумленість зображень і зменшує межі розрядності обчислювальних процедур.

6. Розроблене на основі отриманих теоретичних результатів дисертаційного дослідження програмне рішення забезпечує збереження інформації не лише при передаванні її комунікаційними каналами, а й у випадку організації стійкого персоніфікованого захисту.

7. Модифіковані архітектури для виділених основних класів автоматизованих систем завдяки імплементації розробленої інформаційної технології забезпечують автоматизацію процедур забезпечення функціональної безпеки передавання інформації комунікаційними каналами інформаційно-управляючих систем критичного застосування.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Kovalchuk A. A blend of algorithms RSA and bit, additive-difference operations and algorithmsin El-Gamal images / [A. Kovalchuk, Y. Borzov, D. Peleshko та ін.] // Journal of Global Research in Computer Science. – 2013. – P.1-7.

2. Ковальчук А. Бінарні операції та елементи алгоритму RSA при шифруванні-дешифруванні кольорових зображень/ А.Ковальчук, Д. Пелешко, Ю. Борзов. // Комп'ютерні науки та інформаційні технології. Вісник НУ ЛП – 2013. – №771. – С. 121-125.

3. Ковальчук А. Сумісне використання систем Ель-Гамалята алгоритму RSA в захисті графічної інформації / А.Ковальчук, Д. Пелешко, Ю. Борзов // Комп'ютерні науки та інформаційні технології. Вісник НУ ЛП. 2013.– № 751. – С. 178-182.

4. Борзов Ю. О. Модифікація алгоритму RSA: шифрування та дешифрування за одним рядком матриці зображення / Ю. О. Борзов, А. М. Ковальчук, Д. Д. Пелешко // Науковий вісник НЛТУ України: зб. наук.-техн. праць.– 2012.– Вип. 22.6.– С. 336 - 340.

5. Ковальчук А. Використання побітових операцій і додаткового зашумлення в алгоритмі RSA при шифруванні-дешифруванні зображень / А.Ковальчук, Д. Пелешко, Ю. Борзов// Комп'ютерні науки та інформаційні технології. Вісник НУ ЛП – 2012.– №744.– С. 132-136.

6. Про одну модифікацію алгоритму RSA шифрування-дешифрування півтонових зображень / А. Ковальчук, Д. Пелешко, М. Навитка, Ю. Борзов // Комп'ютерні науки та інформаційні технології. Вісник НУ ЛП – 2012. – №732.– С. 225-229.

7. Використання побітових операцій при шифруванні-дешифруванні кольорових зображень у модифікаціях алгоритму RSA / А.Ковальчук, Д. Пелешко, М. Навитка, Ю. Борзов // Комп'ютерні науки та інформаційні технології. Вісник НУ ЛП – 2011. – №719. – С. 133-136.

8. Поєднання алгоритму RSA і побітових операцій при шифруванні-дешифруванні зображень / А. Ковальчук, Д. Пелешко, М. Хомин, Ю. Борзов // Комп'ютерні науки та інформаційні технології. Вісник НУ ЛП – 2011.– №694.– С. 309-312.

9. Рак Т. Є. Лінійні форми з елементами алгоритму RSA і додаткове зашумлення в захисті півтонових зображень/ Т.Є Рак, Ю.О. Борзов // Науковий вісник НЛТУ України: зб. наук.-техн. праць.– 2015.– Вип. 25.3.– С. 336-340.

10. Use of the bitwise operations for colorimages encryption and decryptionin the RSA algorithm modification/ A.Kovalchuk, D.Peleshko, Y.Borzov, M.Navytka // Proceeding sof the VII IthInternational Scientific and Technical Conference ["Computer Science and Information Technologies" (CSIT 2011)], (Lviv, 16-19November 2011) / Lviv Polytechnic National University. – Lviv: LvivPolytechnic, 2011. – P. 17-18.

11. Шифрування-дешифрування напівтонових зображень модифікаціями алгоритму RSA / А. М. Ковальчук, Д. Д. Пелешко, М. Л. Навитка, Ю. О. Борзов // [Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту], Матеріали міжнародної наукової конференції (Євпаторія, 27-31 травня, 2012) / ХНТУ. – Херсон, 2012. – С. 447-449.

12. Ковальчук А. М. Бінарні операції в алгоритмі шифрування RSA / А. М. Ковальчук, Д. Д. Пелешко, Ю. О. Борзов // [Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту], Матеріали міжнародної наукової конференції (Євпаторія, 16-20 травня, 2011) / ХНТУ. – Херсон, 2011. – С. 358-360.

# АНОТАЦІЯ

**Борзов Ю.О. Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування. – Рукопис.**

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології. – Львівський державний університет безпеки життєдіяльності, Львів, 2015.

Дисертація присвячена розробці інформаційних технологій підвищення функціональної безпеки інформаційно-управляючих систем критичного застосування, які базуються на комунікаційних процедурах, з метою мінімізації обчислювальних ресурсів в процесах забезпечення надійності, стійкості та безпеки функціонування цих систем.

У роботі з використанням операторів зашумлення, елементів криптографічних кодувань Ель-Гамаля і RSA отримано декілька методів що лягли в основу інформаційних технологій забезпечення функціональної безпеки в інформаційно-управляючих системах критичного застосування. Використання процедур, побудованих на основі розроблених методів підвищує, функціональну безпеку телекомунікаційних процедур у випадку використання в мережевих транзакціях у якості інформаційного пакету цифрових зображень різного типу.

Отримали подальший розвиток інформаційні технології забезпечення безпеки для випадку обміну в мережевому середовищі систем критичного застосовування напівтонових зображень із глибиною кольору в 1-2 байти.

Реалізовано спеціалізовані програмні засоби забезпечення підвищення функціональної безпеки при використанні об'єктом комунікації напівтонових та повноколірних зображень. На основі цих засобів розроблено програмний примітив мережевої автоматизованої системи критичного застосування, яка підтримує процес захищеного обміну зображеннями в телекомунікаційних сеансах.

*Ключові слова:* інформаційні технології, автоматизовані системи критичного застосування, функціональна безпека, напівтонові та повноколірні зображення, системи криптографічних кодувань, функція зашумленості, ентропія.

## АННОТАЦИЯ

**Борзов Ю.О. Информационные технологи повышения функциональной безопасности систем обработки информации критического применения. – Рукопись.**

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.06 – информационные технологии. – Львовский государственный университет безопасности жизнедеятельности, Львов, 2015.

Диссертация посвящена разработке информационных технологий повышения функциональной безопасности информационно-управляющих систем критического применения, основанные на коммуникационных процедурах, с целью минимизации вычислительных ресурсов в процессах обеспечения надежности, устойчивости и безопасности функционирования этих систем.

Совместное использование операторов зашумления, элементов систем криптографического кодирования Эль-Гамаля и RSA позволило получить метод повышения функциональной безопасности при передаче в коммуникационных процедурах цифровых изображений с глубиной цвета до 4 байт, который характеризуется высокой криптостойкостью.

Использование элементов метода RSA и операции зашумления позволило получить метод для повышения функциональной безопасности в процедурах защиты полутоновых изображений с глубиной цвета в 1-2 байта, который обладает повышенной устойчивостью к несанкционированному доступу в коммуникационных процедурах автоматизированных систем критического применения.

Усовершенствованная информационная технология функциональной безопасности при транзакциях полутоновых изображений с глубиной цвета в 1-2 байта благодаря использованию элементов алгоритма RSA и поразрядных операций дает возможность обеспечить полную зашумленность изображений и уменьшения границ разрядности вычислительных процедур.

В процессе диссертационных исследований разработаны специализированные программные средства обеспечения повышения функциональной безопасности при использовании объектами коммуникации полутоновых и полноцветных изображений. На основе этих средств разработан программный примитив сетевой автоматизированной системы критического применения, которая поддерживает процесс защищенного обмена изображениями в телекоммуникационных сеансах.

Модифицированы архитектуры основных классов систем критического применения. Благодаря имплементации разработанной информационной технологии в информационно-управляющих системах критического применения, построенных на основании этих архитектур, удалось автоматизировать процедуры информационной безопасности повышенного уровня стойкости.

*Ключевые слова:* информационные технологии, автоматизированные системы критического применения, полутоновые и полноцветные изображения, шифрование изображений, криптографические системы, шумовая функция, энтропия.

## SUMMARY

**Borzov Yu. O.** Information technologies of increase the functional safety of critical application information processing systems. – Manuscript.

Dissertation for a Candidate degree in Technical sciences by specialty 05.13.06 - Information Technologies. − Lviv State University of Life Safety, 2015.

The thesis is devoted to development of information technologies to increase the functional safety information of critical application control systems that are based on communication procedures to minimize the computing resources in the process of reliability, stability and security of these systems.

Based sharing operators noise and cryptographic elements encodings El Gamal and RSA received several methods underlying the information technology ensuring functional safety information in control systems of critical application.

Using procedures, based on the developed methods to increases telecommunication functional safety in network transactions that are use information package in form of digital images of various types.

Further developed information technology security for the case of a network environment sharing of critical application grayscale images with color depth of 1-2 bytes.

Implemented specialized software to ensure increased security in the use of functional object communication and full-color halftone images. Based on these primitive software tools developed network of automated system of critical application that supports the secure exchange process images in telecommunication sessions..

*Keywords:*information technology, automated systems critical applications, functional safety, information security and full-color grayscale images cryptographic system, function noisiness, entropy.