ISSN 2519-2310 (Online)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н.КАРАЗІНА
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
COMPUTER SCIENCE AND CYBERSECURITY
(CS&CS)

№ 1(27) 2025
Issue 1(27) 2025

Заснований 2015 року

Міжнародний електронний науково-теоретичний журнал
International electronic scientific journal

УДК 004(051)

Засновник і видавець Харківський національний університет імені В.Н. Каразіна Міністерства освіти і науки України. Засновано у 2015 році. Періодичність виходу –2 рази на рік.

В журналі публікуються наукові статті з теоретичних і науково-технічних проблем, що пов'язані зі створенням ефективних засобів комп'ютерних інформаційно-комунікаційних систем та питань захисту інформації, на основі передових математичних методів, інформаційних технологій і технічних засобів.

Схвалено до розміщення в мережі Інтернет Вченою радою Харківського національного університету імені В.Н. Каразіна (30.06.2025 р., Протокол № 17).

DOI (Онлайн): **10.26565/2519-2310-2025-1**.

Редакція:
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 6, офіс 315а, Харків, 61022, Україна (*Північний корпус університету, 3 поверх*)

Електронна пошта: cscsjournal@karazin.ua
Веб-сторінка: http://periodicals.karazin.ua/cscs (Open Journal System)

Автори опублікованих матеріалів несуть повну відповідальність за достовірність наведених фактів, власних імен тощо. Опубліковані статті пройшли внутрішнє та зовнішнє рецензування.

UDC 004(051)

Founder and publisher V.N. Karazin Kharkiv National University of the Ministry of Education and Science of Ukraine. Established in 2015. Published 2 times a year.

The journal publishes research articles on theoretical, scientific and technical problems of effective facilities development for computer information-communication systems and information security questions based, on advanced mathematical methods, information technologies and technical means.

Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (June 30, 2025, Protocol No.17).

The journal has Digital Object Identifier: **10.26565/2519-2310-2025-1** (Online).

Editorial office:
V.N. Karazin Kharkiv National University
Svobody Sq., 6, office 315a, Kharkiv, 61022, Ukraine (*North building of University, 3th floor*)

E-mail: cscsjournal@karazin.ua
Web-page: http://periodicals.karazin.ua/cscs (Open Journal System)

The authors of the published materials are solely responsible for the selection, accuracy of the facts, proper names, etc. Published articles have been internally and externally peer reviewed.

ЗМІСТ

CONTENTS

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 1 (27)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 1 (27)

DOI: https://doi.org/10.26565/2519-2310-2025-1-01
УДК 004.056.5

ОЦІНКА ТА ПОРІВНЯННЯ КРИПТОПЕРЕТВОРЕНЬ ТИПУ ЕЛЕКТРОННИЙ ПІДПИС ДОДАТКОВОГО КОНКУРСУ NIST США «DIGITAL SIGNATURE SCHEMES»

Іван Горбенко[1], доктор технічних наук, професор, e-mail: i.d.gorbenko@karazin.ua,
ORCID: https://orcid.org/0009-0003-6979-8946
Єлизавета Острянська[1], молодший науковий співробітник, e-mail: antelizza@gmail.com,
ORCID: https://orcid.org/0000-0003-1412-8470
Володимир Пономар[1], старший науковий співробітник, e-mail: Laedaa@gmail.com,
ORCID: https://orcid.org/0000-0001-5271-2251
[1]*Харківський національний університет імені В.Н. Каразіна,*
майдан Свободи, 4, Харків, 61022, Україна
Рукопис надійшов 1 березня 2025 р. Отримано після рецензування 1 квітня 2025 р.
Прийнято 2 травня 2025 р.

Анотація: У сучасному світі розвиток квантових обчислень ставить під загрозу класичні криптографічні алгоритми, зокрема RSA, EC-DSA та DSA, які використовуються для забезпечення цифрової безпеки. Це створює необхідність розробки постквантових криптографічних рішень, здатних протистояти атакам квантових комп'ютерів. Особливо важливими є стійкі алгоритми електронного підпису, адже вони забезпечують автентифікацію, цілісність та незаперечність інформації у фінансових, юридичних та державних системах. У статті проведено аналіз та порівняння криптографічних схем електронного підпису, що беруть участь у додатковому конкурсі NIST «Digital Signature Schemes». Досліджено ключові математичні основи цих алгоритмів, зокрема криптографію на решітках, схеми на основі кодів, багатовимірні перетворення, ізогенії еліптичних кривих та методи MPC-in-the-Head. Оцінено їхню продуктивність, безпеку та ефективність у контексті постквантових загроз. Проведено детальний аналіз розмірів відкритих ключів, підписів та швидкості операцій генерації ключів, підписання й перевірки. Виявлено основні переваги та недоліки кожного з підходів, визначено перспективні напрями розвитку постквантових електронних підписів та їх можливе практичне застосування. Дослідження є актуальним у зв'язку з необхідністю переходу на нові криптографічні стандарти, що гарантуватимуть безпеку даних у майбутньому. Отримані результати дозволяють оцінити сильні та слабкі сторони розглянутих алгоритмів, а також визначити перспективні напрями подальшого розвитку постквантової криптографії.

Ключові слова: *постквантова криптографія, NIST PQC, електронний підпис, квантово-стійкий, квантово-безпечний*

Як цитувати: Горбенко І., Острянська Є., Пономар В. Оцінка та порівняння криптоперетворень типу електронний підпис додаткового конкурсу NIST США «Digital Signature Schemes». *Комп'ютерні науки та кібербезпека.* 2025; № 1(27): С. 6–16. https://doi.org/10.26565/2519-2310-2025-1-01

In cites: Gorbenko I., Ostrianska Ye., Ponomar V. (2025). Evaluation and comparison of cryptographic digital signature transformations of the additional NIST competition «Digital Signature Schemes». *Computer Science and Cybersecurity. 1*(27): 6–16. https://doi.org/10.26565/2519-2310-2025-1-01 (in Ukrainian)

1. Вступ

У сучасному цифровому світі електронні підписи відіграють ключову роль у забезпеченні автентичності, цілісності та незаперечності інформації. Вони використовуються у фінансових транзакціях, електронному документообігу, цифрових сертифікатах, блокчейн-технологіях та багатьох інших сферах. Так, наприклад, і в Україні вже впроваджено стандарт квантово-стійкого електронного підпису ДСТУ 9212:2023 [4]. Однак із розвитком квантових технологій постає новий виклик – традиційні криптографічні алгоритми можуть стати вразливими до атак квантових комп'ютерів. Саме тому криптографія на решітках є перспективним напрямком досліджень, який активно розвивається в останні роки.

У зв'язку з цим Національний інститут стандартів і технологій США (NIST) запустив ініціативу з розробки нових, стійких до квантових атак електронних підписів (ЕП). Окрім основного конкурсу, NIST також організував додатковий відбір алгоритмів електронного підпису, який включає нові перспективні розробки, що можуть стати альтернативою вже відібраним кандидатам [3]. Цей процес є важливим для забезпечення максимальної безпеки та ефективності майбутніх криптографічних стандартів і він спрямований на оцінку нових перспективних алгоритмів, які можуть забезпечити стійкість до атак квантових комп'ютерів. NIST розглядає різні підходи до побудови постквантових підписів, зокрема криптографію на основі решіток, кодів, багатовимірних рівнянь, ізогеній еліптичних кривих та інтерактивних доказів знання.

Метою цієї роботи є оцінка та експериментальний порівняльний аналіз математичних методів криптоперетворень типу ЕП, які повинні бути стійкими згідно національних вимог до квантовостійких стандартів криптографічних перетворень ЕП та конкурсу NIST США «Digital Signature Schemes». У цій статті також розглянуто принципи роботи електронних підписів, та аналізуються найбільш перспективні алгоритми, що претендують на роль майбутніх криптографічних стандартів.

2. Попередні визначення та критерії порівняння

На даний момент після більш, ніж року оцінювання, NIST обрав 14 алгоритмів-кандидатів ЕП (див. табл. 1) для другого раунду додаткового конкурсу електронних підписів для процесу стандартизації NIST PQC [1].

Критерії для визначення кандидатів у першому раунді включали положення щодо еталонного та оптимізованого коду C, тести з відомими відповідями, письмову специфікацію та необхідні заяви про інтелектуальну власність. Це були єдині критерії, за якими оцінювали пакети подання. Інші фактори, такі як безпека, вартість і характеристики алгоритму та реалізації кандидатів, не враховувалися під час процесу перевірки перед першим раундом, а також криптоаналіз або дані продуктивності подання не вплинули на прийняття кандидатів у першому раунді.

Вже для другого раунду NIST [2] визначив три широкі аспекти критеріїв оцінки, які будуть використовуватися для порівняння алгоритмів-кандидатів на роль підпису в рамках процесу стандартизації NIST PQC: 1) безпека, 2) вартість і продуктивність і 3) характеристики реалізації. Також схеми повинні суттєво відрізнятися від схем підписів, які NIST вже вибрав для

стандартизації. Зокрема, в умовах конкретно зазначено, що подання повинні, як мінімум, відповідати одному з наступних критеріїв:

• Схеми на основі решітки повинні забезпечувати принаймні одну велику перевагу в продуктивності порівняно зі вже стандартизованими Crystals-Dilithium і Falcon.

• Алгоритми, що не базуються на решітці, повинні забезпечувати принаймні одну велику перевагу в продуктивності над SPHINCS+.

Щодо безпекових критеріїв відбору, то NIST перерахував бажані властивості безпеки, такі як стійкість до бічних каналів і атак з кількома ключами та стійкість до неправильного використання. У поданнях заохочувалося зазначати додаткові бажані властивості безпеки, надані крім стандартної непідробності (наприклад, ексклюзивне право власності, підписи в повідомленні та можливість повторного підписання). Нарешті, NIST вимагав узагальнення відомих криптоаналітичних атак на схеми та оцінку складності цих атак.

Другим за важливістю критерієм під час оцінки потенційних алгоритмів були вартість і продуктивність, зокрема, розмір відкритих ключів і підписів та обчислювальна ефективність операцій підписання та перевірки, а також генерації ключів (тобто швидкість алгоритмів). Вимоги до пам’яті стосуються як розміру коду, так і вимог до оперативної пам’яті (RAM) для програмних реалізацій.

Таблиця 1 – Схеми ЕП другого раунду конкурсу NIST

Table 1 – Digital signature schemes of the 2nd round of the NIST competition

№	Підпис Signature	Математична основа Mathematical foundation
1.	CROSS	Коди/Codes
2.	LESS	
3.	SQIsign	Ізогенії/Isogenies
4.	HAWK	Алгебраїчні решітки/ Algebraic lattices
5.	Mirath (об’єднання MIRA/MiRitH)	MPC-in-the-Head
6.	MQOM	
7.	PERK	
8.	RYDE	
9.	SDitH	
10.	MAYO	Багатовимірні перетворення/ Multidimensional transformations
11.	QR-UOV	
12.	SNOVA	
13.	UOV	
14.	FAEST	Симетричні перетворення/ Symmetric transformations

Серед кандидатів, визначених в таблиці 1: два алгоритми ЕП на основі кодів, один алгоритм ЕП на основі ізогеній, один алгоритм ЕП, в основі якого лежать операції на решітках, п’ять кандидатів на роль алгоритму ЕП на основі методу MPC-in-the-Head та чотири алгоритми, в основі яких лежать багатовимірні перетворення. На основі симетричних криптоперетворень було обрано одну схему електронного підпису.

3. Короткий огляд алгоритмів підписів

CROSS (Codes and Restricted Objects Signature Scheme) [5] – це постквантова схема електронного підпису, що базується на кодах, розроблена для забезпечення безпеки в умовах квантових обчислень. Вона використовує структури кодів та обмежених об'єктів для створення стійких до квантових атак підписів. Ця схема підпису отримана шляхом застосування перетворення Фіата-Шаміра до інтерактивного протоколу ідентифікації з нульовим знанням (ZK). CROSS базується на так званій проблемі декодування обмеженого синдрому (R-SDP), NP-складній задачі, яку можна розглядати як варіант класичної проблеми декодування синдрому (SDP). Хоча немає поки відомих атак проти CROSS, проблеми відносно нові. NIST чекає подальшого аналізу основних проблем і протоколу ідентифікації ZKPoK. CROSS пройшов до другого раунду частково через зацікавленість NIST у ньому як у схемі «не на решітках», яка демонструє переваги продуктивності порівняно з SLH-DSA.

LESS [6] – це криптографічна схема, що використовує кодові структури для забезпечення безпеки в умовах квантових обчислень. Вона розроблена для створення стійких до квантових атак електронних підписів, використовуючи складність декодування лінійних кодів. LESS будується шляхом застосування перетворення Фіата-Шаміра до інтерактивного ZKPoK розв'язку задачі еквівалентності обчислювального коду. Безпека LESS базується на складності проблеми лінійної еквівалентності (LEP). У результаті було отримано дуже гнучку схему, яка пропонує для кожного рівня безпеки кілька компромісів між простотою, швидкістю, розміром відкритого ключа та розміром підпису. Крім того, параметри легко вибирати та масштабувати.

SQIsign [7] – це постквантова схема електронного підпису, що базується на ізогеніях суперсингулярних еліптичних кривих. Вона використовує математичні властивості ізогеній для забезпечення безпеки та компактності підписів. Як і кілька інших кандидатів, SQIsign використовує парадигму Фіата-Шаміра, щоб перетворити схему ідентифікації з нульовим знанням на схему підпису. Безпека базується на знанні секретної ізогенії еліптичної кривої. SQIsign має новий підхід, і тому потребує додаткової оцінки та аналізу. NIST сподівається, що додаткові дослідження призведуть до подальшої оптимізації, яка покращить продуктивність.

HAWK [8] – це схема підпису типу hash-and-sign на основі решітки, яка тісно пов'язана з Falcon. Центральними математичними об'єктами в HAWK є матриці елементів з одного сімейства кілець, які використовуються в алгоритмах на основі решітки, обраних для стандартизації. Falcon використовує швидке перетворення Фур'є, яке використовує арифметику з плаваючою комою. HAWK покладається на проблему найкоротшого вектору (omSVP) і проблему ізоморфізму решітки модуля пошуку (smLIP), щоб уникнути витоку секретної інформації. NIST вирішив залишити HAWK на 2-й раунд через його високу ефективність.

Mirath [9] (злиття MIRA та MiRitH) – це схема електронного підпису, заснована на складності вирішення проблеми MinRank. MIRA і MiRitH – це схеми підписів, створені на парадигмі багатосторонніх обчислень (MPCitH). Підписи для обох схем генеруються шляхом застосування перетворення Фіата-Шаміра до ZKPoK розв'язку задачі MinRank. Безпека як для MIRA, так і для MiRitH базується на складності проблеми MinRank. Ці схеми містять варіанти, які використовують структуру гіперкубу, яка є оптимізацією в рамках парадигми MPCitH, яка використовує додатковий обмін секретами, що дозволяє розпаралелювати протокол MPCitH.

MQOM [10] – це схема підпису, побудована на парадигмі MPCitH, яка базується на складності розв'язання випадкової багатовимірної системи квадратних рівнянь з рівною кількістю змінних і рівнянь. Незважаючи на те, що проблема вирішення багатовимірних квадратичних систем була добре вивчена, нещодавні результати можуть мати незначний вплив на її параметри, необхідні для досягнення цільових рівнів безпеки. Як і інші схеми, що базуються на методах «in the head», MQOM забезпечує дуже малі розміри відкритих ключів і

середній розмір підписів. NIST вважає, що зміни в другому раунді допоможуть знайти оптимальні компроміси між продуктивністю та розмірами підписів на основі різних припущень складності.

PERK [11] – це схема електронного підпису, заснована на складності вирішення проблеми PERmuted Kernel. Вона розроблена для забезпечення безпеки від атак як класичних, так і квантових комп’ютерів. PERK – підпис, який складається із ZKPoK секретної перестановки. Хоча проблема, на яку спирається PERK, була запропонована близько 30 років тому, існує невизначеність щодо її конкретної складності. Додаткові дослідження цього припущення допоможуть підвищити впевненість у конкретних параметрах PERK для різних рівнів безпеки.

RYDE [12] – схема підпису, побудована на парадигмі MPCitH. Подібно до інших схем підпису MPCitH, побудова RYDE передбачає генерування випадкового рівняння разом із рішенням. NIST висунув RYDE до другого раунду конкурсу через конкурентоспроможність схеми в категорії схем підписів MPCitH і VOLEiTH. Основна складна проблема декодування синдрому рангу також виглядає неструктурованою, а відповідне припущення щодо безпеки виглядає консервативним.

Syndrome Decoding in the Head (SDitH) [13] – базується на структурі MPCitH і пропонує набори параметрів з використанням двох методів оптимізації. Тобто схема SDitH має два варіанти: варіант гіперкуба і пороговий варіант. Безпека базується на складності розв’язання d-розподіленого варіанту проблеми декодування синдрому для випадкових лінійних кодів над кінцевими полями. Незважаючи на те, що SDitH тісно пов’язаний із відомою NP-складною проблемою, NIST вважає, що SDitH може отримати користь від аналізу безпеки.

MAYO [14] – це варіант UOV з меншими відкритими ключами. Відновлення ключа MAYO зводиться до пошуку простору «oil» UOV, а підробка підпису MAYO зводиться до спроби інвертувати відображення, схоже на UOV. Завдяки цій додатковій структурі MAYO значно покращує розмір відкритого ключа порівняно з UOV, успадковуючи малий розмір підпису UOV. Хоча він не такий швидкий, як UOV, MAYO все ще дуже ефективний.

QR-UOV [15] є варіантом UOV з меншими відкритими ключами з використанням фактор-кільця. На відміну від матриць UOV, елементи яких належать скінченному полю . Завдяки додатковій структурі відкритий ключ QR-UOV на 50% менший порівняно з UOV. NIST зберігає інтерес до QR-UOV через його конкурентоспроможність, але структура QR-UOV потребує подальшого вивчення. NIST передбачає, що продуктивність може бути покращена, і заохочує розробників до подальшої оптимізації їх впровадження.

Алгоритм електронного підпису SNOVA [16] є варіантом алгоритму UOV, який зберігає характеристику коротких підписів UOV, водночас пропонуючи меншу довжину відкритого ключа порівняно з традиційним алгоритмом UOV, що забезпечує переваги як у аспектах безпеки, так і в ефективності електронних підписів. Під час першого раунду SNOVA зазнала атаки, яка вплинула на деякі з поданих наборів параметрів. Потім SNOVA оновила свої параметри, але зазнала нової атаки. Тим не менш, деякі з представлених наборів параметрів SNOVA перенесли обидві атаки. Новизна SNOVA та історія її атак змушують NIST поставити під сумнів її безпеку навіть більше, ніж інші схеми структурованого UOV, спрямовані на значно зменшений розмір ключа. Проте той факт, що SNOVA все ще має безперебійні набори параметрів із найменшими відкритими ключами, доступними для схем на основі UOV, робить його привабливим кандидатом для продовження вивчення

UOV (Unbalanced Oil and Vinegar) [17] – це схема електронного підпису, яка залишається безпечною навіть проти квантових комп’ютерів. Схема UOV є найстарішою безперервною багатовимірною криптосистемою, яка була запропонована в 1999 році. Структура UOV базується на системі квадратних рівнянь, для якої існує секретний підпростір, на якому

система оцінюється як нуль. Ця схема забезпечує безпеку EUF-CMA. Хоча UOV є зрілою та досить стабільною схемою, атака за останні чотири роки незначно знизила безпеку деяких режимів її параметрів. NIST рекомендує суспільству залишатися пильним і продовжувати критично аналізувати безпеку UOV.

FAEST [18] – це схема електронного підпису, створена за допомогою відносно нової техніки під назвою VOLEitH. Ця техніка пов'язана з підходом MPCitH, який використовується кількома іншими схемами підписів у процесі постквантової стандартизації NIST. Хоча теоретична безпека FAEST базується лише на припущеннях симетричного ключа, його продуктивність значно краща, ніж у більшості інших схем із такою властивістю, включаючи SLH-DSA. Однак продуктивність FAEST не конкурентоспроможна зі схемами на основі решітки, такими як ML-DSA і FN-DSA. Таким чином, FAEST є багатообіцяючою схемою для програм, які не вимагають продуктивності, що забезпечується підписами на основі решітки.

4. Порівняльний аналіз підписів

У цьому розділі у таблицях 2-6, відповідно, наведено результати порівняння розмірів підписів, відкритих ключів, а також швидкодію розглянутих в попередньому розділі підписів додаткового конкурсу NIST. Порівняння було проведено для 1, 3 та 5-го рівнів безпеки NIST відповідно. Усі значення розмірів ключів і підписів в таблицях 2-6 наведено в байтах, а швидкодія в – у циклах процесору. В таблиці 2 розглянуто порівняння алгоритмів на кодах.

Таблиця 2 – Порівняння схем ЕП на кодах

Table 2 – Comparison of code-based schemes performance

Схема	Параметри	Відкритий ключ (байти)	Підпис (байти)	Генерація ключів (цикли)	Підписання (цикли)	Верифікація (цикли)
CROSS	R-SDP(G)-1-f	54	9120	130,000	3,713,000	2,125,000
	R-SDP(G)-3-f	83	22464	140,000	5,630,000	3,530,000
	R-SDP(G)-5-f	106	40100	165,000	11,756,000	7,448,000
LESS	LESS-1-252	67484	1745	1,300,000	94,400,000	93,500,000
	LESS-3-400	35074	5585	4,000,000	336,800,000	365,100,000
	LESS-5-548	85793	9464	10,000,000	981,200,000	998,000,000

В таблиці 3 наведено порівняння алгоритмів на MPC-in-the-Head перетвореннях. Запуски алгоритмів та середні оцінки часу було здійснено та розраховано на комп'ютері на процесорі Intel Core i9-13900K на 3 GHz з використанням AVX2 інструкцій. Також слід зазначити, що схема SDitH розглядалася для варіанта гіперкуба, а інші схеми в таблиці 3 розглядалися в швидкому варіанті.

Таблиця 3 – Порівняння схем на MPC-in-the-Head перетвореннях

Table 3 – Comparison of MPC-in-the-Head-based schemes performance

Схема	Параметри	Відкритий ключ (байти)	Підпис (байти)	Генерація ключів (цикли)	Підписання (цикли)	Верифікація (цикли)
Mirath	Mirath-1a-Fast	73	3,728	200,000	11,000,000	9,800,000
	Mirath-3a-Fast	107	8,537	300,000	33,600,000	34,400,000
	Mirath-5a-Fast	147	15,507	500,000	86,700,000	65,100,000
RYDE	RYDE-1-Fast	69	3,597	35,900	6,700,000	6,600,000

	RYDE-3-Fast	101	8,264	64,700,000	27,300,000	27,100,000
	RYDE-5-Fast	133	14,609	77,500,000	49,000,000	44,500,000
SDitH	gf256-L1-hyp	132	8,496	14,200,000	10,800,000	9,700,000
	gf256-L3-hyp	180	19,544	16,600,000	26,200,000	22,900,000
	gf256-L5-hyp	244	33,924	28,700,000	49,900,000	44,000,000
PERK	PERK-I-fast5	240	8,030	89,000	7,000,000	4,900,000
	PERK-III-fast5	370	18,000	186,000	15,000,000	11,000,000
	PERK-V-fast5	510	31,700	324,000	33,000,000	26,000,000
MQOM	L1-gf251-fast	59	7809	480,000	11,520,000	10,160,000
	L3-gf251-fast	92	17161	1,960,000	32,850,000	29,580,000
	L5-gf251-fast	125	29919	4,830,000	81,550,000	75,580,000

Нижче в таблиці 4 розглянуто порівняння алгоритмів на багатовимірних перетвореннях, тобто схем, в основі яких лежить принцип UOV. Для схеми UOV ми розглядали класичний варіант, для схеми MAYO для рівня безпеки NIST I було розглянуто набір параметрів MAYO_one, який має менші відкриті ключі та більший розмір підпису, а також було обрано варіант, що має AVX2 оптимізації. Щодо схеми підпису QR-UOV, то було розглянуто еталонну реалізацію на коді C з AVX2 інструкціями та AES PRG для наборів параметрів (q,v,m,l): (127,156,54,3), (127,228,78,3), (127,306,105,3). Для алгоритму SNOVA в таблиці в дужках зазначено, що до розміру підпису/відкритого ключа додатково додається +16 байт солі/початкового значення, відповідно.

Таблиця 4 – Порівняння схем ЕП на багатовимірних перетвореннях

Table 4 – Comparison of multivariate schemes performance

Схема	**Параметри**	**Відкритий ключ (байти)**	**Підпис (байти)**	**Генерація ключів (цикли)**	**Підписання (цикли)**	**Верифікація (цикли)**
UOV	uov-I-classic	412,160	128	4,203,437	105,324	90,336
	uov-III-classic	1,225,440	200	17,603,360	299,316	241,588
	uov-V-classic	2,869,440	260	49,490,856	591,812	470,886
MAYO	I	1420	454	216,704	872,216	392,541
	III	2986	681	362,446	1,676,585	665,382
	V	5554	964	910,684	3,582,362	10,737,685
QR-UOV	I	24,255	200	8,587,000	1,586,000	1,224,000
	III	71,891	292	32,311,000	4,599,000	3,410,000
	V	173,676	392	95,579,000	10,504,000	7,463,000
SNOVA	I	9,826(+16)	90(+16)	9,595,012	10,964,945	3,161,199
	III	31,250(+16)	136(+16)	44,658,255	47,587,816	9,443,639
	V	71,874(+16)	188(+16)	166,196,633	158,443,732	25,289,616

В таблиці 5 розглянемо єдину схему підпису на решітках додаткового конкурсу NIST, а саме HAWK та порівняємо її зі схемою Falcon, що також в основі має математику на решітках. Вона використовує швидке перетворення Фур’є для підписання повідомлення та покладається на проблему найкоротшого вектору (omSVP). Для HAWK та Falcon ми розглядаємо параметри для I (HAWK-512) та V (HAWK-1024) рівнів безпеки NIST та робили тести з використанням AVX2 інструкцій.

Таблиця 5 – Порівняння схем ЕП на алгебраїчних решітках

Table 5 – Comparison of lattice-based schemes performance

Схема	Параметри	Відкритий ключ (байти)	Підпис (байти)	Генерація ключів (цикли)	Підписання (цикли)	Верифікація (цикли)
HAWK	HAWK-512	1024	555	8,432,840	85,371	156,224
	HAWK-1024	2440	1221	43,660,958	190,936	314,625
Falcon	1	897	666	19,872,000	1,009,764	81,036
	5	1793	1280	63,135,000	2,053,080	160,596

В таблиці 6 розглянуто схеми FAEST та SQISign, що базуються на симетричних перетвореннях та ізогеніях, відповідно. Обидві схеми ЕП використовують перетворення Фіата-Шаміра для протоколу з нульовим знанням та мають малі розміри відкритих ключів, але, як показано в таблиці 6 нижче, є дуже повільними, особливо в порівнянні зі схемами на решітках.

Таблиця 6 – Порівняння схем FAEST та SQISign

Table 6 – Comparison of FAEST and SQISign schemes performance

Схема	Параметри	Відкритий ключ (байти)	Підпис (байти)	Генерація ключів (цикли)	Підписання (цикли)	Верифікація (цикли)
FAEST	FAEST-128f	32	4,506	5,000	12,787,000	9,783,000
	FAEST-192f	40	11,260	11,000	54,687,000	42,290,000
	FAEST-256f	48	20,696	13,000	76,330,000	74,546,000
SQISign	I	65	148	43,300,000	401,600,000	5,100,000
	III	97	224	134,000,000	899,200,000	18,600,000
	V	129	292	212,000,000	1,207,500,000	35,700,000

Таким чином, розглянувши окремо порівняння алгоритмів на різних математичних конструкціях (табл. 2-6), для повноти дослідження на рис. 1 ми наводимо їх загальне порівняння.

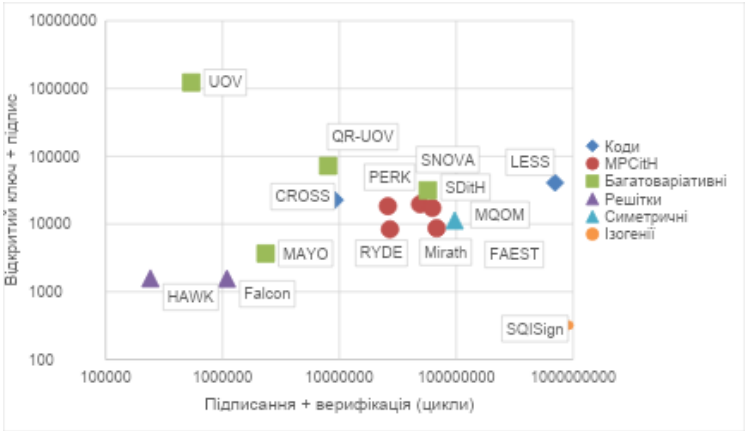


Рис. 1 – Порівняння алгоритмів підпису за співвідношенням відкритий ключ+підпис та час підписання+верифікації

Fig. 1 – Comparison of signature algorithms by public key+signature length ratio and signing+verification time

В результаті аналізу алгоритмів підпису з рис.1 можна зробити висновки, що кожен із підходів має власні переваги та обмеження, які необхідно враховувати при розробці стандартів криптографічного підпису.

Щодо розміру відкритих ключів та підписів, то найменший розмір підпису в сумі з довжиною відкритого ключа спостерігається у схемі на основі ізогеній (SQISign). Також доволі невеликі відкриті ключі та підписи демонструють схеми на основі MPC-in-the-Head перетворень (MQOM, RYDE, Mirath), що робить їх привабливими для застосувань із обмеженими ресурсами. Натомість, найбільші відкриті ключі характерні для UOV та SNOVA, що може бути значним недоліком у реальних сценаріях використання. Хоча в той же час UOV має дуже короткі підписи та високу швидкість підписання та перевірки. Найменший розмір підпису в сумі з довжиною відкритого ключа забезпечує SQIsign, тоді як у CROSS та PERK підписи є значно більшими.

Найшвидші алгоритми для створення підпису та верифікації – схеми, в основі яких лежать перетворення на алгебраїчних решітках і це HAWK (і Falcon), але схеми на основі багатовимірних перетворень, такі як UOV та MAYO, також демонструють непогану швидкість підписання, що робить їх ефективними для великомасштабних операцій. Схеми на кодах такі як CROSS і LESS, мають нижчу продуктивність у процесі підписання через складні обчислення. Але вони потрапили до другого раунду частково через зацікавленість NIST у них як у схемах «не на решітках», що демонструють переваги продуктивності порівняно з SLH-DSA. Щодо схеми SQIsign на основі ізогеній, то генерація підпису є повільнішою порівняно з іншими кандидатами через складність математичних конструкцій, і таким чином є складним для впровадження.

Якщо розглядати алгоритми з точки зору безпеки та стійкості до атак, то схеми на основі кодів (CROSS, LESS) вважаються безпечними, але потребують додаткового аналізу з точки зору довготривалої стійкості. А також їх структура є доволі специфічною тому, реалізація може бути складною, що вимагає ретельного підходу та експертизи HAWK та інші схеми на решітках використовують перевірені математичні припущення, але можуть бути уразливими до атак бічними каналами.

Окремо виділяється схема FAEST на основі техніки VOLEitH. Хоча теоретична безпека FAEST базується лише на припущеннях симетричного ключа, його продуктивність значно краща, ніж у більшості інших схем із такою властивістю, включаючи SLH-DSA. Основна техніка VOLEitH, що лежить в основі схеми була представлена тільки в 2023. Конструкція дещо складна та нова, а надійність безпеки дуже технічна. Тому спільності криптографів та науковців необхідний час, щоб впевнитися в безпеці даної конструкції.

Схема на основі ізогеній (SQIsign) вимагає оптимізації та глибшого аналізу криптостійкості через складну структуру. Інші схеми підпису, особливо на багатовимірних перетвореннях, покладаються на добре вивчені проблеми, такі як MinRank, Rank-SD, тощо, і є стійкими до квантових атак, але деякі з них потребують додаткового криптоаналізу.

6. Висновки

1. Дослідження алгоритмів електронного підпису, що беруть участь у другому раунді додаткового конкурсу NIST [3], дозволяє оцінити їхні сильні та слабкі сторони з точки зору безпеки, продуктивності та ефективності реалізації. Конкурс спрямований на доповнення основного процесу стандартизації, забезпечуючи різноманітність криптографічних підходів, які можуть бути використані в постквантовому середовищі.

Другий раунд додаткового конкурсу NIST представляє важливий крок у розробці постквантових алгоритмів електронного підпису. Алгоритми, що базуються на

MPC-in-the-Head, демонструють високу продуктивність та ефективність, тоді як схеми на решітках, кодах та багатовимірних перетвореннях мають потенціал завдяки своїм унікальним властивостям та багаторічному криптоаналізу, тобто надійній стійкості до квантових атак.

Успішна стандартизація та впровадження постквантових підписів у сучасні криптографічні системи є критично важливим завданням для забезпечення довготривалої безпеки цифрових технологій. Тому було розглянуто кандидатів на електронний підпис та проведено порівняльний аналіз. В результаті можна сказати, що NIST зацікавлений в альтернативах схемам на алгебраїчних решітках, бо шукає нові рішення та конструкції для різних застосувань. Перспективами подальшого розвитку поточних досліджень є:

• Оптимізація розміру підписів та ключів: хоча багато алгоритмів демонструють гарну продуктивність, зменшення їх розмірів без втрати безпеки залишається ключовим завданням.

• Зміцнення стійкості до комбінованих атак: деякі алгоритми, особливо на основі кодів та багатовимірних перетворень, потребують додаткових перевірок та більш глибокого криптоаналізу проти нових атак.

• Практичне впровадження: багато алгоритмів поки що не мають ефективних реалізацій, оптимізованих для апаратних платформ та мобільних пристроїв і тому процес впровадження є складним.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

References

1. Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process (2024). *NIST Internal Report NIST IR 8528* https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8528.pdf
2. National Institute of Standards and Technology (2022) *Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process*. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf
3. National Institute of Standards and Technology (2025) *Post-Quantum Cryptography: Additional Digital Signature Schemes Round 2 Additional Signatures*. https://csrc.nist.gov/projects/pqc-dig-sig/round-2-additional-signatures
4. Information Technologies. Cryptographic Information Protection (2023) Electronic Signature Algorithm on Algebraic Lattices with Deviations: DSTU 9212:2023. Kyiv: Derzhspozhyvstandart of Ukraine [in Ukrainian]
5. CROSS – Codes and Restricted Objects Signature Scheme (2025) *Submission to the NIST Post-Quantum Cryptography Standardization Process*. https://www.cross-crypto.com/CROSS_Specification_v2.0.pdf
6. Baldi M. and others (2025) LESS. *Linear Equivalence Signature Scheme.* https://www.less-project.com/LESS-2025-02-07.pdf
7. Marius A. and others (2025) SQIsign. *Algorithm specifications and supporting documentation*. Version 2.0. URL:. https://sqisign.org/spec/sqisign-20250205.pdf
8. Joppe W. Bos and others (2025) *HAWK*. Version 1.1. URL: https://hawk-sign.info/hawk-spec.pdf
9. Agj G. and others (2025) Mirath Signature Scheme *Algorithm Specifications and Supporting Documentation.* URL: https://pqc-mirath.org/assets/downloads/mirath_v2.0.pdf.
10. Feneuil Th. Rivain M (2023) MQOM: MQ on my Mind *Algorithm. Specifications and Supporting Documentation* (Version 1.0). URL: https://mqom.org/docs/mqom-v1.0.pdf
11. Aaraj Na. and others (2025) PERK. Version 2.0. URL: https://pqc-perk.org/assets/downloads/perk-v2.0.pdf
12. Aragon N. and others. RYDE Signature Scheme. *Algorithm Specifications and Supporting Documentation.* Version 2.0. URL: https://pqc-ryde.org/assets/downloads/ryde_specification_v2.0.pdf

13. Melchor C. A. and others (2023) The Syndrome Decoding in the Head (SD-in-the-Head) Signature Scheme. *Algorithm Specifications and Supporting Documentation* – Version 1.1. URL: https://sdith.org/docs/sdith-v1.1.pdf
14. Beullens W. and others (2023) MAYO. *Algorithm Specifications*. URL: https://pqmayo.org/assets/specs/mayo.pdf.
15. Hiroki Furue and others (2025) QR-UOV. *Algorithm Specifications*. Nippon telegraph and telephone corporation. URL: https://info.isl.ntt.co.jp/crypt/qruov/files/qruov_Spec-v2.0.pdf
16. SNOVA (2023) Proposal for NIST PQC: Digital Signature Schemes project. Version 1.0. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/SNOVA-spec-web
17. Beullens W. and others (2023) UOV: Unbalanced Oil and Vinegar. *Algorithm Specifications and Supporting Documentation.* Version 1.0. URL: https://drive.google.com/file/d/1NdMHuCyyFG6xgOGrpssM99kyiNwA9JG-/view
18. Baum C. and others (2025) FAEST v2: *Algorithm Specifications*. Version 2.0. URL: https://faest.info/faest-spec-v2.0.pdf.

EVALUATION AND COMPARISON OF CRYPTOGRAPHIC DIGITAL SIGNATURE TRANSFORMATIONS OF THE ADDITIONAL NIST COMPETITION «DIGITAL SIGNATURE SCHEMES»

Ivan Gorbenko[1], Doctor of Sciences (Engineering), Full Prof.; e-mail: i.d.gorbenko@karazin.ua;
ORCID: https://orcid.org/0000-0003-6979-8946
Yelyzaveta Ostrianska[1], junior researcher; e-mail: antelizza@gmail.com;
ORCID: https://orcid.org/0000-0003-1412-8470
Volodymyr Ponomar[1], senior researcher fellow; e-mail: Laedaa@gmail.com;
ORCID: https://orcid.org/0000-0001-5271-2251
[1] *V. N. Karazin Kharkiv National University, Ukraine*
Manuscript was received March 1, 2025; Received after review April 1, 2025;
Accepted May 2, 2025

Abstract. In the modern world, the development of quantum computing threatens classical cryptographic algorithms, in particular RSA, ECDSA and DSA, which are used to ensure digital security. This creates a need to develop post-quantum cryptographic solutions that can be resistance under quantum computers attacks. Stable digital signature algorithms are especially important, as they provide authentication, integrity and non-repudiation of information in financial, legal and government systems. The article analyzes and compares cryptographic digital signature schemes participating in the NIST supplementary competition "Digital Signature Schemes". The main mathematical foundations of these algorithms are investigated, in particular, lattice cryptography, code-based schemes, multivariate transformations, elliptic curve isogenies and MPC-in-the-Head methods. Their performance, security and efficiency in the context of post-quantum threats are assessed. A detailed analysis of the length of public keys, signatures and the speed of key generation, signing and verification operations is carried out. The main advantages and disadvantages of each approach are identified, promising directions for the development of post-quantum digital signatures and their possible practical application are identified. The research is relevant in connection with the need to transition to new cryptographic standards that will guarantee data security in the future. The results allow to assess the strengths and weaknesses of the considered algorithms, as well as to identify promising directions for the further researches of post-quantum cryptography.

Keywords: *post-quantum cryptography; NIST PQC, digital signature, quantum-resistant; quantum safe*

Conflicts of Interest: the authors declare no conflict of interest.

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 1 (27)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 1 (27)

DOI: https://doi.org/10.26565/2519-2310-2025-1-02
УДК 004.93+621.39

SPEECH TECHNOLOGY FOR CONTROLLING ELECTRONIC DEVICES

Mhnd Farhan[1], Lecturer at Department of Electrical Engineering, Faculty of Engineering,
e-mail: mhndfarhan@yahoo.com, ORCID: https://orcid.org/0009-0007-0541-6995
[1]*Baghdad University, Iraq*

Manuscript was received April 20, 2025; Received after review May 23, 2025;
Accepted June 29, 2025

Abstract: This paper presents a system that employs the use of speech technology to control electronic devices attached to PCs. The work in this paper is implemented in two major phases. Phase one is the software part of the system. Its role is to accept voice signals from a microphone attached to the PC and perform speech recognition on the signal, determine operating commands from the recognized phrases and control devices attached to the computer ports. Phase two is a hardware logic circuit connected between the PC's printer port and the devices being controlled. This logic circuit which is implemented using simple logic gates performs addressing and control mode for the electronic devices being controlled. The system runs on windows vista operating system and it is capable of authenticating users and validating their action. User response for the system is provided in both voice response and graphic display messages.

Keywords: *Voice Control, multiple devices, speech*

In cites: Mhnd Farhan (2025). Speech Technology for Controlling Electronic Devices. *Computer Science and Cybersecurity.* 1(27): 17–32. https://doi.org/10.26565/2519-2310-2025-1-02

1. Introduction

Speech is one of the most natural ways to interact. If an application can be controlled solely by way of voice commands then the opportunity that lies is unlimited. Even though the idea of using speech as an input mechanism for an application is not new, there are not a lot of applications that use speech as input. In other words speech is still a big opportunity that is yet to be explored [1-3]

Most people currently are very busy as they strive to achieve their life long dreams and ambitions. As a result they hardly have time to go about normal routines at home, office, train stations or bus stops etc. This has led to high demand for automation of most domestic appliances. Speech is the latest technology which has now arrived at our door steps [4-8].

In addition to having access to digital electronic domestic appliances, at least one in every two households has a computer. Most modern homes boast of numerous and vast rooms. With our busy schedules voice control of domestic devices comes in handy especially with the emergence of Bluetooth audio transceivers. One can now control domestic appliances without necessarily being close to them [9-10].

The main objective of this paper is to develop a system which would allow voice input to control and monitor multiple electronic devices. The system is PC based. It makes use of the PC

microphone, speech recognition technology, and PC communication ports such as parallel port or any other data communication ports available in the PC. This concept presents an opportunity to any individual who has a PC and may wish to use voice as an input to control electronic devices around them.

2. Design methodology

A. Software design

This software implements Automated Speech Recognition(ASR) command interpretation and execution. It receives its input from a microphone connected to the PC. It is driving and manipulating the parallel port. It is also responsible for installing and maintaining information on the domestic appliances being controlled. The software in order to carry out its functions is implemented under the following modules.

- VoiceControl.Core
- VoiceControl.DataAccess
- VoiceControl.Port
- VoiceControl.ParallelportUtility
- VoiceControl.Security
- VoiceControl.Service
- VoiceControl.Speech
- VoiceControl.UI(User Interface)

Each of the modules is dedicated to unique tasks that eventually build up to the overall software application. Fig.1 shows the interaction between modules.

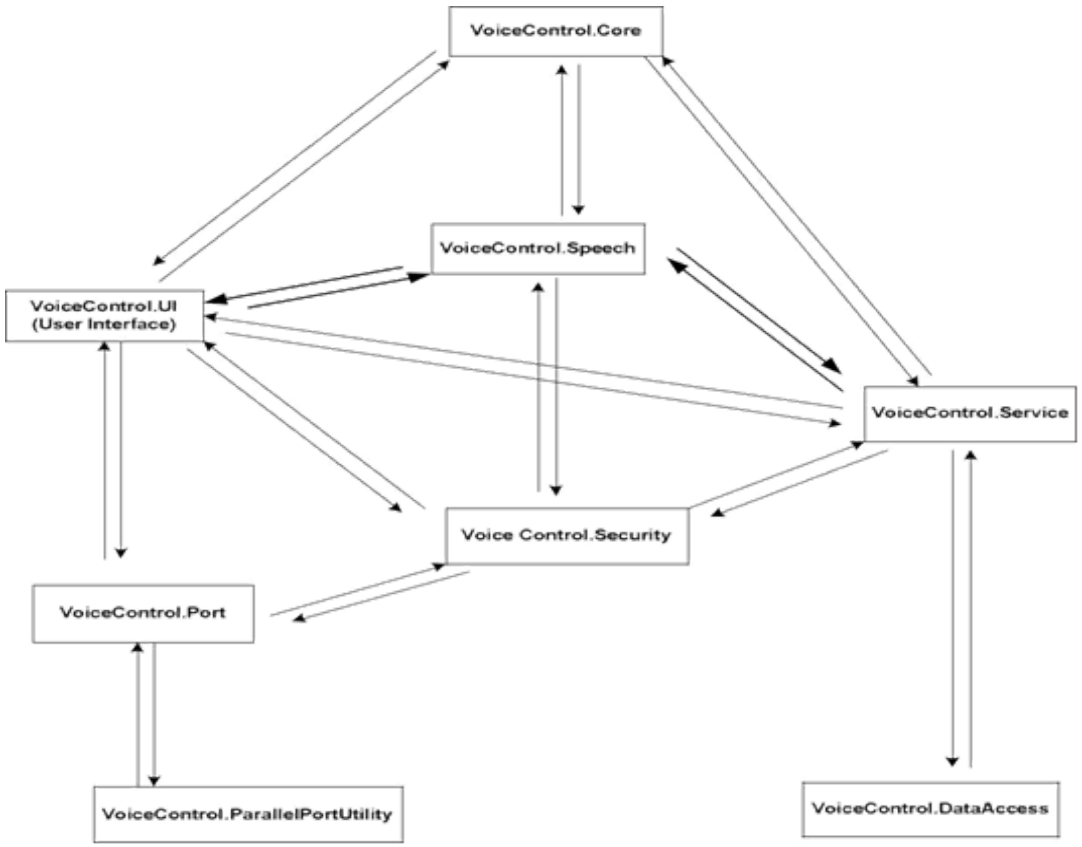


Fig. 1 – Interaction between modules

A-1. System Function

1 - VoiceControl.Core

VoiceControl.Core is responsible for modeling systems objects and all the domestic appliances to be driven by the application.

2 - VoiceControl.DataAccess

VoiceControl.DataAccess tasks involve manipulation of system objects stored in the database. It is charged with establishing a connection to the database, inserting, retrieving, deleting and updating database objects.

3 - VoiceControl.Port

This module contains class objects that model both the serial port and parallel port. The port module provides serial or parallel port class instances which are used to create serial port or parallel port. These therefore access and initiate the actual PC ports for transmission or reception of data.

4 - VoiceControl.ParallelportUtility

This utility module contains the functions which are used to address parallel ports (LPT). It is basically charged with reading or writing to the port. Manipulation of printer ports is a bit complex unlike serial port. To manage LPT ports, the application employs the use of native code in order to directly access registers in the PC which are dedicated to the ports. The application then opens and writes binary or hex data type to the port depending on the operation to be executed.

5 - VoiceControl.Security

In this module, both systems and application level security are implemented. That is for the application level security, authentication of system users is done. On the other hand, it validates every action the user performs on the system. The module verifies whether a particular user is granted permission to perform a certain function. It then either allows or denies the user access to that function.

6 - VoiceControl.Service

The service module is basically an abstraction of the data access module. This acts as a coupling layer between the user interface (UI) and data access module. In this case it has to be loosely coupled allowing for independence of each module and seamless interaction between the calling module and data access module.

7 - VoiceControl.Speech

The speech module provides the means by which input voice signals are recognized and the system's operation command extracted. It also employs the use of voice response to provide feedback to the user.

8 - VoiceControl.UI (User Interface)

This is the graphical user interface (GUI) module. It's basically responsible for providing the user interactivity front for the system. It contains forms with control buttons on it. The user is expected to provide some of the input response through these controls.

A-2. System Users

The voice control system manager is appointed to manage and maintain the devices and the system process data. The user requires basic training on how to use the system and is assumed to be familiar with computers, the Microsoft Windows operating system and commonly used Microsoft Windows microphone input devices. The user’s voice is equally trained to increase the accuracy of single word error rate (SWER) engine.

A-3. System Requirements

1 - Operating System

The application is designed to operate on Microsoft Windows Operating System 2000 or higher. (Windows XPSP3, Windows Vista) with the necessary service packs applied.

2 - Database System

The application uses the Microsoft SQL Server (MSDE) 2000 or Microsoft SQL Server 2005 express or higher as the database platform.

3 - Runtime Environment

The application runs on the Windows.NET runtime version 3.0 or higher. The application is developed and complied in C# .NET. The computer on which the application is installed requires that a supported version of the runtime to be installed. The software natively installs the required runtime.

4 - Hardware

Any computer hardware capable of running the above mentioned system environment is suitable for the application. The system however requires enough hard disk space to accommodate the application database.

A-4. Software Features

The application is designed and developed under the following category.

1 - VoiceControl.Core

- Class Rule
- Class Gate
- Class Light
- Class Phone
- Class PhoneBook
- Class PhoneCall
- Class Radio
- Class ShortMessage

2 - VoiceControl.DataAccess

- Class ActionDAO
- Class DataAccessUtility
- Class GateDAO
- Class IDAO
- Class LightDAO
- Class PhoneBookDAO
- Class PhoneDAO

- Class RadioDAO
- Class SpeechStateDAO
- Class UserDAO
- Class UserGroupDAO
- Class VoiceGrammarDAO
- Class VoiceParallelPortDAO
- Class VoicePPPinDAO
- Class VoiceSerialPortDAO

3 - VoiceControl.Port

- Class VoiceParallelPort
- VoicePPPin
- Class VoiceSerialPort

4 - VoiceControl.Security

- Class Action
- Class User
- Class UserGroup

5 - VoiceControl.Service

- Class ActionService
- Class GateService
- Class LightService
- Class PhoneBookService
- Class PhoneService
- Class RadioService
- Class SpeechService
- Class SpeechStateService
- Class UserService
- Class UserGroupService
- Class VoiceGrammarService
- Class VoiceParallelPortService
- Class VoicePPPinService
- Class VoiceSerialPortService

6 - VoiceControl.Speech

- Class SpeechState
- Class VoiceGrammar
- Class VoiceSpeechEngine
- Class VoiceSpeechTraining
- Class VoiceTTS

7 - User Interface

The following forms are designed

- Actions Form
- Calls Form
- Commands Form
- Dashboard Form

- Gate Form
- Light Form
- List of Calls Form
- List of Objects Form
- List of Sms Form
- Login Form
- Gate Operations Form
- Light Operations Form
- Phone Operations Form
- Radio Operations Form
- Parallel port Form
- Phone Form
- Phone Book Form
- Parallel port pins Form
- Radio Form
- Serial port Form
- Sms Form
- User Form
- User Group Form

8 - Database Objects

The system has a database where it stores information about all installed devices, their status and also information on the system and system users. Therefore a database is designed and the following are the database objects developed:

- Table of Actions
- Table of Devices
- Table of Gates
- Table of Grammars
- Table of Lights
- Table of PhoneBooks
- Table of Phones
- Table of Radios
- Table of SpeechStates
- Table of UserGroups
- Table of Users
- Table of VoiceParallelPorts
- Table of VoicePPPins
- Table of VoiceSerialPorts

A-5. Software Testing

The application is tested at the following two levels.

1 - Unit Testing

This is done to verify implementation of class functions, procedures and properties. A third party tool known as NUnit is employed for unit testing. This ensures that every function or procedure developed returns the results expected of it.

2 - Integration Testing

This is performed to check the overall performance of the application. The system is tested on how it works or interacts with the port hardware interface, response to user input stress (also known smoke test) and finally it is tested against the database.

B. Hardware Design

B-1. Connecting Circuits to the Parallel Port

PC parallel port is a 25 pin D-shaped female connector at the back of the computer as shown in Fig.2. It is normally used for connecting computers to printers, but many other types of hardware for the port are available today. Not all 25 pins are always needed. Usually one can easily do with only 8 output pins (data lines) and signal ground.

The data pins are transistor-transistor-logic (TTL) level output pins. This means that they output ideally 0V when they are in low logic level (0) and +5V when they are in high logic level (1). In the real world the voltages can be something different from ideal when the circuit is loaded. The output current capacity of the parallel port is limited to only a few milliamperes.

The parallel port usually comes as a 25-pin female port and it is commonly used to connect printers to a computer. Many geeks also use it to connect their own devices to their PCs. There are a few more things to remember when using a PC's parallel port. It can load only 2.5mA and ~2.5 volts. It is better to use opto-couplers or ULN2803 when interfacing with an external device.

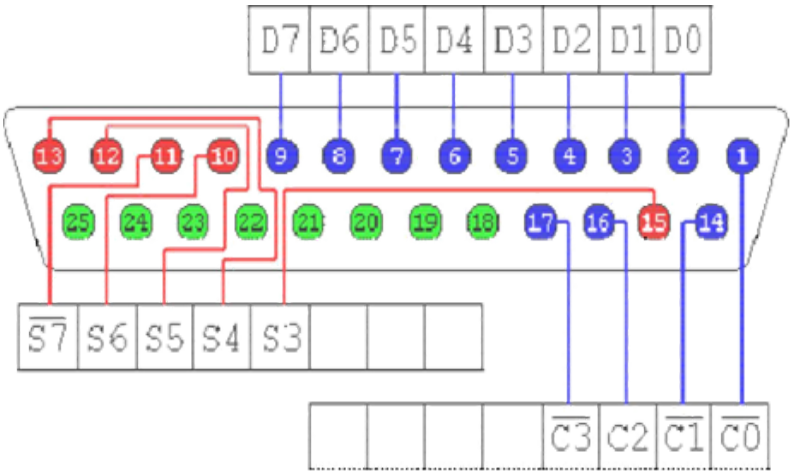


Fig. 2 – Pin out of DB25 connector

1 - Data Register

This is the register that allows the user to write values into the port. In simple words, these pins can be used to output a specific value in a data register. Voltages in specific pins can also be changed. These are called output pins. There are altogether 8 output pins available, ranging from D0 to D7.

2 - Status Register (Pins)

These are called input pins or status registers and can hold a value that the outside world gives to the parallel port. So, this port acts like a reader and it has 5 pins for inputs. The pin range is S4 to S7.

3 - Control Register (Pins)

This register can be used in both ways, it enables a user to write values to the outside world, as well as read values from the outside world. However, we need to remember that most of the control pins work in an inverted manner. We can see them with a dash sign on the top of the pin. Pin range is C0 to C3. Ground pins are used as neutral; these pins are used as (-) in batteries. If we are connecting a device to a parallel port in order to read or write, we have to use one or more ground pins and a read/write pin to work. For example, if we are trying to light up an light-emitting-diode (LED), then we have to connect the (-) of the LED to a ground pin and the (+) of the LED to an output pin. For reading purposes, we use the same mechanism.

4 - Addressing the Parallel Port and Registers

Port addressing control is a great deal in port programming, as it is the door that enables programs to connect to the external circuit or device. In normal PCs, a parallel port address can be one of the addresses given below, but depending on the basic input/output system(BIOS) settings and some other issues, the parallel port address can vary. However, it always lies in one of these address ranges.

- LPT1 03BC (hex) 956(decimal)
- LPT2 0378 (hex) 888(decimal)
- LPT3 0278 (hex) 632(decimal)

5 - How to Light up LEDs

To test the output, assume that we wrote value 2 to the data register and we want to know which pin outputs +5V. The data register starts from pin number 2 and ends in pin number 9, so there are 8 pins for output. In other words, it's an 8-bit register. So, when we write 2 to its data register, +5 voltages will be there in the 3rd pin. We have to take a scientific calculator and convert Decimal 2 to Binary; then the value is 2(DEC) = 1 0(BIN), so 1 0 means ‘000 0 0 0 1 0’ is the status at the data register. When we want to light up an LED, there is a special way to connect them to a data register. Here we have to connect a ground pin to any pin starting from the 18th to 25th. All are ground pins, so there is no difference. The output pin or positive of the LED should be connected to a pin in the data register. When we write a value which enables that particular data register pin, then the LED will light up.

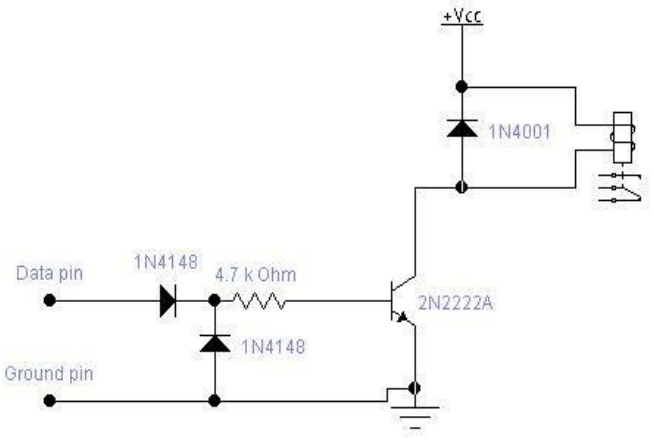


Fig. 3 – Relay controlling circuit

B-2. Relay Circuit

The circuit shown in Fig.3 is used to control the relay from the parallel port.

The circuit needs an external power supply which has the output voltage which is right for controlling the relay (5-24V depending on relay). The transistor does the switching of current and the diode prevents spikes from the relay coil from damaging the computer. Since coils (solenoids and relay coils) have a large amount of inductance, when they are released (when the current is cut off) they generate a very large voltage spike. Hence a diode circuit is used to block that voltage spike from hitting the rest of the circuit. The circuit is then used for controlling the electronic devices.

The 1N4001 diode in parallel with the relay is an essential protection component because damage of the parallel port can occur because of high voltage inductive kickback from the relay coil (the diode stops that spike from occurring).

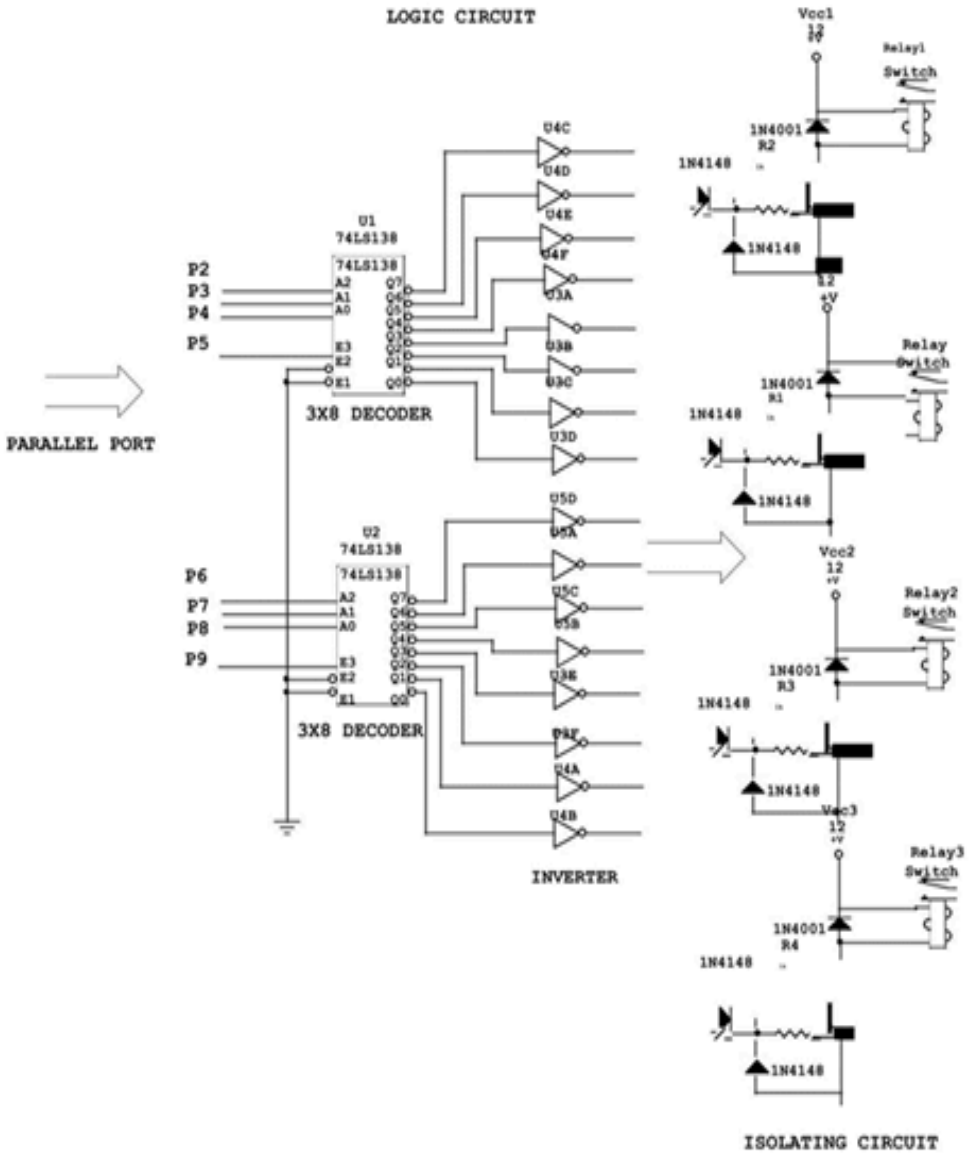


Fig. 4 – Hardware logic circuit

The circuit protects the parallel port against higher than +5V signals and also against wrong polarity signals (power on the circuit is accidentally at wrong polarity).

More safety is added by replacing the 1N4148 diode connected to ground with 5.1V zener diode. That diode will then protect against overvoltage spikes and negative voltage at the same time.

The decoders are used to select the address and control level for a device. The system sends a binary code sequence to the parallel port which is interpreted by the decoder. At the output of the decoder, inverters are connected since the decoders used are active low. The outputs of the inverters are then channeled through circuit with the relay switch which finally drives the devices. The complete hardware logic circuit is shown in Fig.4.

C. System Process

The system in this paper is designed to receive voice signals from the microphone directly connected to the PC .The microphone can be any ordinary microphone compatible with PCs.

The voice/speech which contains control commands is recognized and the command interpreted by the control program. The program is responsible for creating speech grammar from the commands of each device stored in the database. This grammar is then loaded into the speech engine as the basis for recognition.

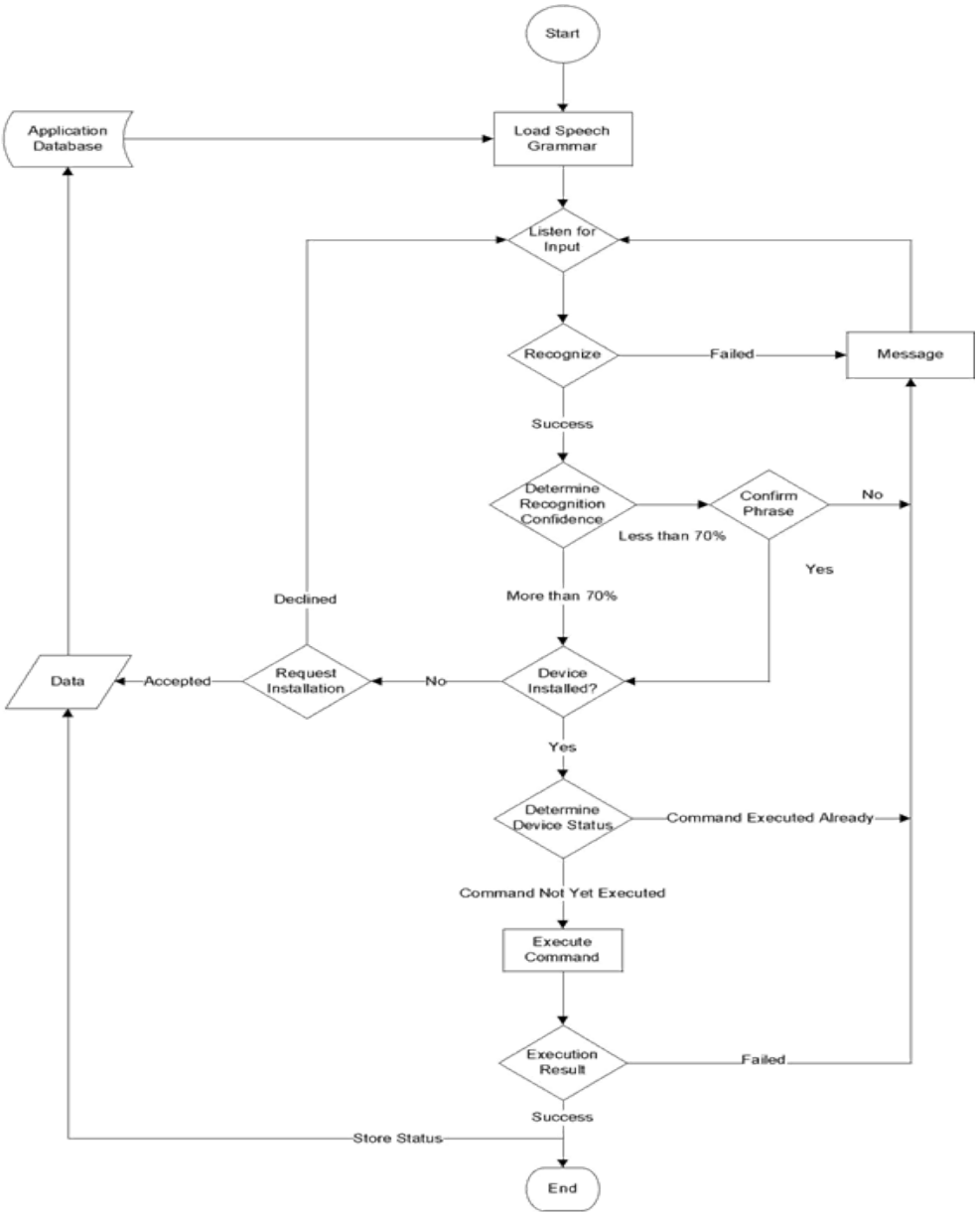


Fig. 5 – Program process chart

The following steps outline the control program's process, while, Fig.5 shows the program process chart.

- The application during start-up initializes the SR engine by loading it with speech grammar. The grammar is created from the operating command phrases stored in the database.
- The application shall then wait for an input signal from the microphone attached to the PC. If voice input is detected it proceeds to 3, otherwise the application will continue waiting for an input.
- The application then initiates speech recognizer instances and parse recognition. If it succeeds the application proceeds to 4, otherwise a system error message is generated and the application goes back to 2.
- Using the initialized recognizer, the application determines the confidence level of the recognized phrase. If it is more than 70% it proceeds to 5, otherwise it goes back to 2.
- The application analyzes the recognized phrase for operating commands. If a command is found, it proceeds to 6, otherwise, it goes back to 2.
- Application determines whether the device to be operated is installed. If so, it proceeds to 7, otherwise it requests for installation of the device and then goes back to 2.
- The system determines the status of the device before executing the operating command. If the command has been executed, a message is generated informing the user that the command had been executed. It then goes back to 2, otherwise, it proceeds to 8.
- The system executes the operating command. If execution of the command succeeds it goes back to 2, otherwise it generates a message indicating an error has occurred then proceeds to 2.

3. Results and analysis

Before the user could speak to the microphone connected to PC with the required command, the system verified whether the user is validated and authenticated .The application verified the user by first confirming if the user existed in the systems database, as shown in Fig.6

Fig. 6 – User login

After validating, it allows the user to log into the system with the existing user profile. The system established users had not undergone voice training as shown in Fig.7 in order to facilitate accurate speech recognition. It then offered the user a speech training session via a wizard developed in the system to take users through speech training as shown in Fig.8.

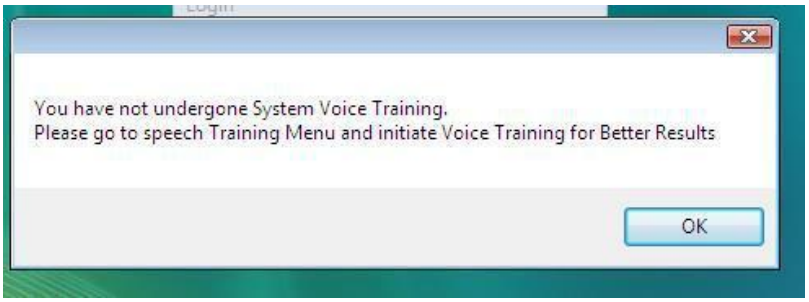


Fig. 7 – Untrained user detected by the application

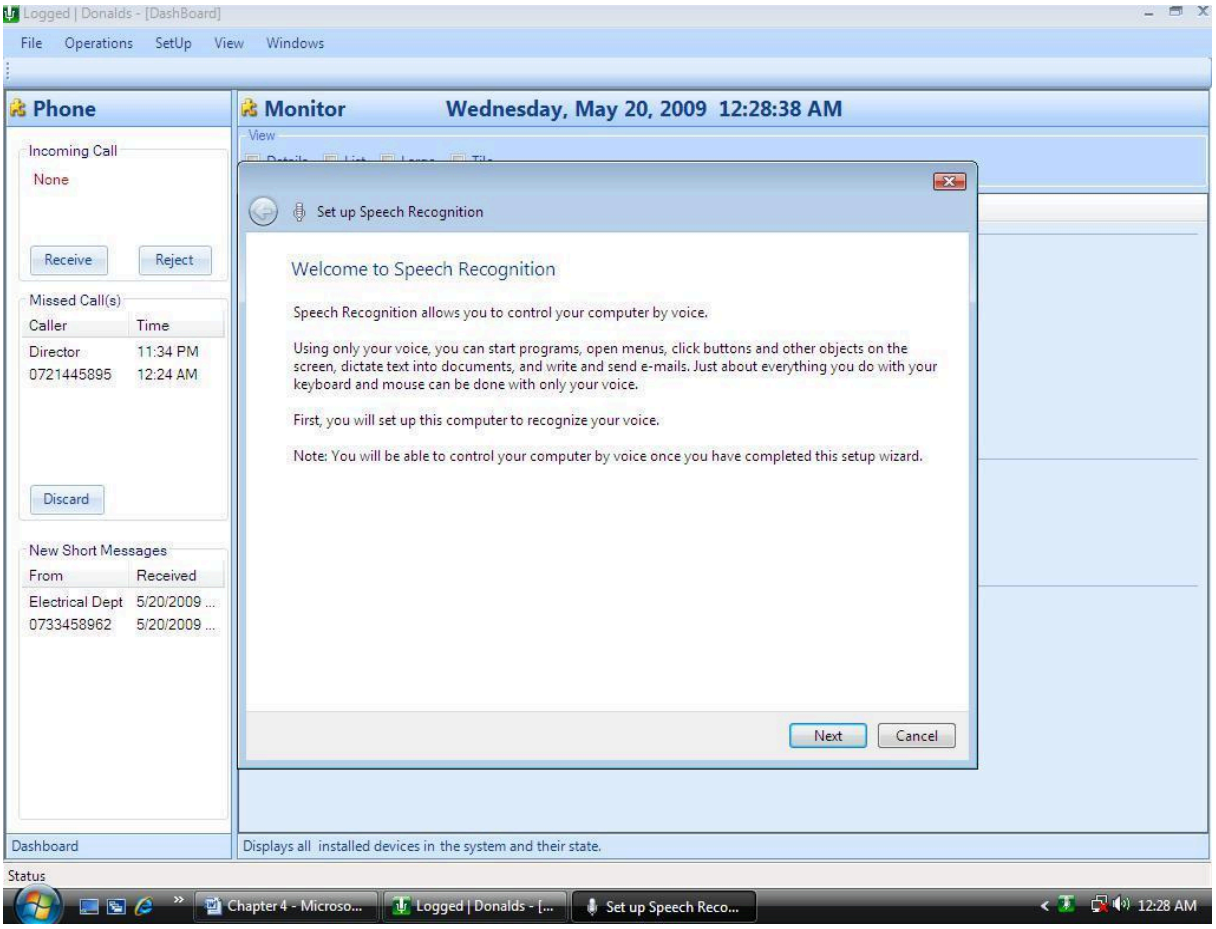


Fig. 8 – Application voice training wizard

Upon completion, the user is allowed to install new devices in the system. This includes bedroom light, sitting room light, a DVD player radio system and a gate. Each of these devices are then assigned operating commands shown in the command table 1. When the system is fully initialized, the user exited graphics thereafter activating speech operating mode for the system as shown in Fig.9.

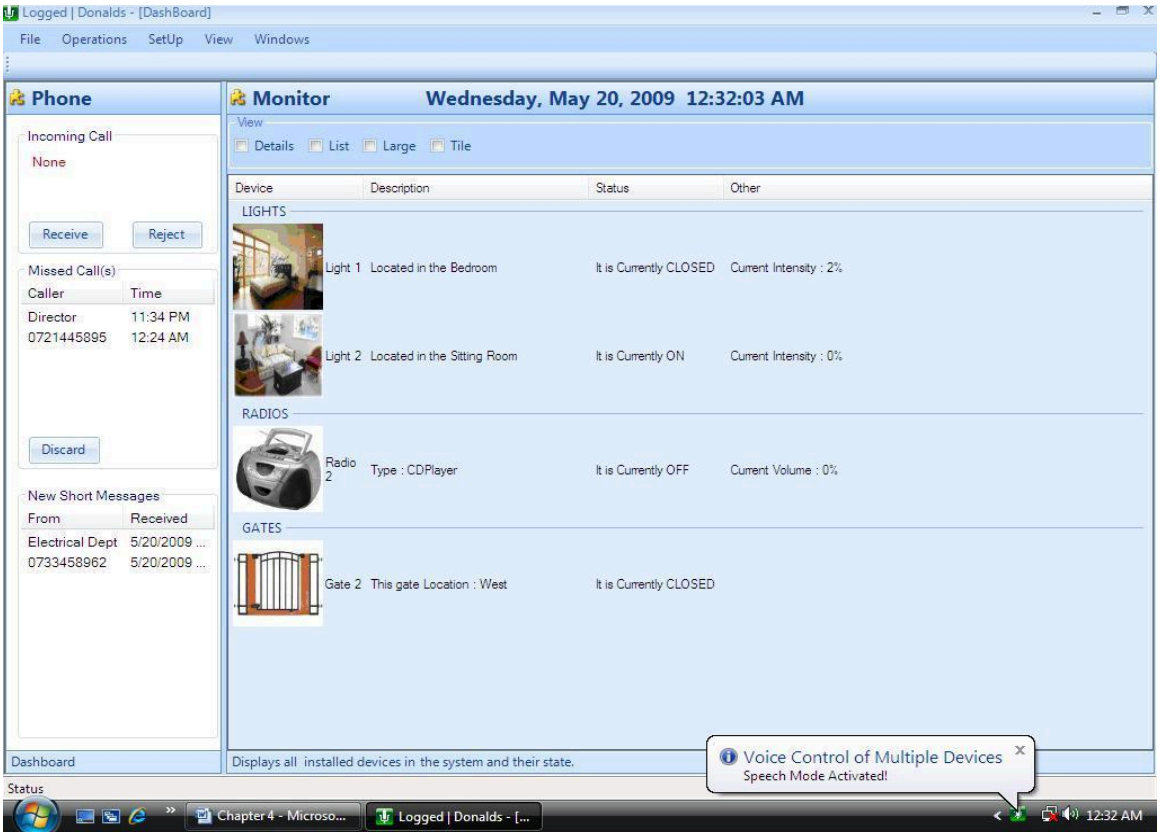


Fig. 9 – Speech activated

The system loaded the speech engine with grammar whose main parameters are the systems installed devices commands and names. When speech is detected in the microphone, the system first establishes its threshold. In order to achieve this, the application uses speech hypothesis to determine the confidence level of the recognized phrase. It then uses the recognized phrase for example, 'Bedroom Light ON', to verify whether such an action is permitted for the user. The user had permission to switch on or off any device. It goes ahead and checks if the light is ON. It was not ON and so the system goes ahead and implements the command. It returns a voice response 'Bedroom Light Switched ON' to the user. Table 2 shows various results.

Table 1. Commands table

DEVICE	COMMANDS	PORT ADDRESS	CONTROL PINS
Bedroom Light	Bedroom Light OFF Bedroom Light ON Increase Bedroom Light Intensity Decrease Bedroom Light Intensity	888	Pin02, Pin08, Pin09, Pin07, Pin06
Sitting room Light	Sitting room Light ON Sitting room Light OFF	888	Pin03, Pin08, Pin09, Pin07, Pin06

Gate 1	Gate 1 OPEN Gate 1 CLOSE	888	Pin05, Pin08, Pin09, Pin07, Pin06
CD Player Radio	Radio ON Radio OFF Increase Radio Volume Decrease Radio Volume	888	Pin04, Pin08, Pin09, Pin07, Pin06

Table 2. Various results

DEVICE	STATUS	RECOGNIZED PHRASE	NEW STATUS	VOICE RESPONSE
Bedroom Light	OFF	Bedroom Light OFF	OFF	Bedroom Light is OFF
	OFF	Bedroom Light ON	ON	Bedroom Light is ON
	50% intensity	Increase Bedroom Light Intensity	60%	Intensity is now 60%
Sitting room Light	ON	Sitting room Light OFF	OFF	Sitting room Light Switched OFF
Gate 1	CLOSED	Open Gate 1	OPENED	Gate 1 Opened
CD Player Radio	OFF	Radio ON	ON	Radio Switched ON
	0% Volume	Increase Radio Volume	10% Volume	Volume is now 10%

4. Conclusions

A speech based voice control of multiple devices was discussed, designed and implemented. The design and implementation was based on connecting a microphone and connecting the electronic appliances through the parallel port. The software was developed to perform automated speech recognition and response operations. The results obtained for the system allowed users to control various home appliances using their voice speaking directly to the microphone attached to the system. The system also allowed the users to get voice response feedback from the system on the accomplishment of the request. The users were also able to inquire and get the status of the various home appliances connected to the system. The user's voice was also able to be trained by the system. Though to keep the application simple, only the bare minimal features of the application were emphasized.

References

1. Mahmud K., Joarder M. and A. Roy A., (2015) "Voice activated electronic devices control system for home appliances". *Scholars Journal of Engineering and Technology,* No.3, pp. 66-70.
2. Amrutha S., Aravind S., Mathew A., Sugathan S., Rajasree R. and Priyalakshmia S., (2015) "Voice controlled smart home", *International Journal of Emerging Technology and Advanced Engineering*, Vol.5, Issue 1
3. Dekate A., Kulkarni C., and Killedar R., (2016) "Study of voice controlled personal assistant device", *International Journal of Computer Trends and Technology*, Vol.42, No.1
4. Kamdar H., Karkera R., Khanna A., Kulkarni P. and Agrawal S., (2017) "A review on home automation using voice recognition", *International Research Journal of Engineering and Technology*, Vol.4, Issue 10
5. Chenxuan H., (2021) "Research on Speech Recognition Technology for Smart Home," 2021 IEEE 4th International Conference on Automation, *Electronics and Electrical Engineering (AUTEEE)*, Shenyang, China, pp. 504-507, DOI: https://doi.org/10.1109/AUTEEE52864.2021.9668828
6. Janíček M., Holubek R., Ružarovský R. and Velíšek K., (2021) "Voice frequency impact for voice control of collaborative robots", *IOP Conf. Ser. Mater. Sci. Eng*., vol. 1009
7. Rane M., Kanade D., Sonone O., Suryawanshi A., Solanka P. and Ghonmode S., (2023) "Voice-Controlled Home Automation System", *Smart Trends in Computing and Communications*. SmartCom, Lecture Notes in Networks and Systems, vol 650. *Springer* DOI: https://doi.org/10.1007/978-981-99-0838-7_14
8. Froiz-Míguez I., Fraga-Lamas P. and Fernández-CaraméS T.M., (2023) "Design, Implementation, and Practical Evaluation of a Voice Recognition Based IoT Home Automation System for Low-Resource Languages and Resource-Constrained Edge IoT Devices: A System for Galician and Mobile Opportunistic Scenarios," in IEEE Access, vol. 11, pp. 63623-63649, DOI: https://doi.org/10.1109/ACCESS.2023.3286391
9. Norda M., Engel C., Rennies J., Appell J.E., Lang S.C. and Hahn A., (2024) "Evaluating the Efficiency of Voice Control as Human Machine Interface in Production," in IEEE *Transactions on Automation Science and Engineering*, vol. 21, no. 3, pp. 4817-4828. DOI: https://doi.org/10.1109/TASE.2023.3302951
10. S. N, S. S and K. K N, (2024) "Voice Controlled Smart Home for Disabled," 2024 *International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics* (IITCEE), Bangalore, India, pp. 1-4, DOI: https://doi.org/10.1109/IITCEE59897.2024.10467328

МОВЛЕННЄВІ ТЕХНОЛОГІЇ КЕРУВАННЯ ЕЛЕКТРОННИМИ ПРИСТРОЯМИ

Моханнад Фархан[1], викладач кафедри електротехніки, інженерний факультет;
e-mail: mhndfarhan@yahoo.com; ORCID: https://orcid.org/0009-0007-0541-6995
[1]*Багдадський університет, Ірак*
Рукопис надійшов 20 квітня 2025 р. Отримано після рецензування 23 травня 2025 р.
Прийнято 29 червня 2025 р.

Анотація: У цій статті представлено систему, яка використовує мовленнєві технології для керування електронними пристроями, підключеними до ПК. Робота в цій статті реалізується у два основні етапи. Перший етап – це програмна частина системи. Його роль полягає в прийнятті голосового сигналу від мікрофона, підключеного до ПК, та виконанні розпізнавання мовлення за сигналом, визначенні робочих команд з розпізнаних фраз та управлінні пристроями, підключеними до портів комп'ютера. Другий етап – це апаратна логічна схема, підключена між портом принтера ПК та керованими пристроями. Ця логічна схема,

реалізована за допомогою простих логічних вентилів, виконує адресацію та режим керування керованими електронними пристроями. Система працює під управлінням операційної системи Windows Vista та здатна автентифікувати користувачів та перевіряти їхні дії. Відповідь користувача для системи надається як голосовою відповіддю, так і графічними повідомленнями.

Ключові слова: *Голосове керування, множина пристроїв, мовлення*

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 1 (27)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 1 (27)

DOI: https://doi.org/10.26565/2519-2310-2025-1-03
УДК 004.738.5

DEVELOPMENT OF A UNIVERSAL ENERGY-EFFICIENT AUTOMATED METER READING SYSTEM USING ESP32-CAM

Tetiana Korobeynikova[1], PhD (Engineering), Associate Professor;
e-mail: tetiana.i.korobeinikova@lpnu.ua; ORCID: https://orcid.org/0000-0003-2487-8742
Oleksandr Reminnyi[1], PhD (Engineering), Assistant; e-mail: sasha.reminnyi@gmail.com;
ORCID: https://orcid.org/0009-0005-5119-3695
Roman Baitala[1], student of the Department of Computerised Automation Systems;
e-mail: roman.baitala.ir.2023@lpnu.ua;
Vladyslav Kyryk[1], student of the Department of Computerised Automation Systems;
e-mail: vladyslav.kyryk.ir.2023@lpnu.ua;
Danylo Stetskyi[1], student of the Department of Computerised Automation Systems;
e-mail: danylo.stetskyi.ir.2023@lpnu.ua
[1]*Lviv Polytechnic National University, Ukraine*
Manuscript was received April 21, 2025; Received after review May 22, 2025; Accepted June 22, 2025

Abstract. The article discusses the design and development of a universal automated meter reading system capable of handling multiple resource types, including water, gas, and electricity. The developed system addresses common challenges associated with manual meter reading, such as accessibility, inconsistent data recording, and human error. The primary innovation presented is integrating the ESP32-CAM module to automate image capturing and data transmission to utility services through a user-friendly mobile application. Special emphasis is placed on optimizing energy efficiency to ensure extended device autonomy. The proposed system includes a robust algorithm for image preprocessing, meter reading validation, and secure wireless communication. Rigorous testing across Android and iOS platforms demonstrated the application's usability, functionality, and consistent performance. Optimization efforts significantly improved device battery life from approximately 50 days to four months. Future improvements are suggested, including developing a custom hardware board to reach the industry-standard operational duration of one year.

Keywords: *automated meter reading, ESP32-CAM, IoT, energy efficiency, mobile application, neural network, utility management*

In cites: Korobeynikova T., Reminnyi O., Baitala R., Kyryk V., Stetskyi D. (2025). Development of a universal energy-efficient automated meter reading system using ESP32-CAM. *Computer Science and Cybersecurity.* 1(27): 33–40. https://doi.org/10.26565/2519- 2310-2025-1-03

1. Introduction

Today, more than ever before, society strives to make life easier and automate all possible processes. Moreover, process automation is gaining momentum, which has caused the appearance of

new devices with a relatively large number of advantages, such as high autonomy of work, accuracy, speed of work, and others [1–3].

One of these devices is devices or smart meters that automatically read indicators and transmit them to utility services without human intervention. These devices and smart meters help people. They have quite a lot of advantages. But its main problem is the price. This field is growing quickly, so we chose it to develop our device that would help people read meters and transmit them to utilities [4–5]. Also, a rather significant drawback of the devices currently offered on the market was that the device could transmit only one type of energy, i.e., water, gas, or electricity. That's why we made our solution universal. And can interact with any counter. This feature is our main advantage after the price.

2. Problem statement

Today, numerous solutions allow customers to monitor data on resource consumption, such as gas, water, and electricity. However, there are a lot of old meters that will enable only manual data entry. One of the main issues is the difficulty of consistently recording meter readings. Many people forget to take these readings regularly [6–7]. As a result, the process is often delayed or neglected, leading to accumulated debt or billing discrepancies. Another significant issue is the accessibility of meters. Many meters are located in inconvenient or remote places, which makes accessing them challenging. Even if the customer manages to get readings, the issue of submitting data to a service provider remains [8]. Human error can also play a role because individuals might mistakenly enter incorrect values and, as a result, get inaccurate calculations and potentially higher bills [9–10]. The primary feature of the system described in this work is its ability to automate the entire process of collecting meter readings. This system eliminates the need for consumers to record data manually. It captures readings at regular intervals, reducing the situation when customers forget to get readings.

Purpose: to develop a universal hardware-software solution for automated meter reading and data visualization, ensuring reliability, convenience, and prolonged device operation.

Object: automated meter reading systems for utilities (water, gas, electricity).

Subject: methods and technologies for automatically capturing, processing, and transmitting meter data.

Methods and tools: the system integrates hardware and software methodologies, utilizing the ESP32-CAM microcontroller, deep-sleep power optimization techniques, image preprocessing algorithms, neural network-based optical character recognition (OCR), and secure wireless communication via Wi-Fi and Bluetooth. Kotlin Multiplatform was employed to create a unified, cross-platform mobile application with rigorous functional, usability, and performance testing.

This work aims to create a hardware device that will take photos of your meter and a software application to interpret data taken from photos to charts. Another essential requirement is the device's lifetime because it must be on a high level for comfortable usage. Its battery should last a long time to keep the device running smoothly and reduce the need for frequent upkeep, giving users a worry-free experience. The final application should deliver a complete and automated data collection and monitoring solution. This system will allow users to quickly see their consumption without repeating the task of manual data submission, ensuring accuracy and timely updates to billing information and eliminating the risk of billing discrepancies.

3. Algorithm for taking data from counter

The algorithm for reading and processing data from counters integrates both hardware and software functionalities to ensure seamless operation:

1. Activation: The device activates once a month, following a predefined schedule.
2. Image Capture: The ESP32-CAM module captures an image of the meter display. The

device ensures proper alignment and clarity using auto-focus or fixed-focus settings optimized during setup.

3. Preprocessing: The captured image undergoes preprocessing via the onboard processor, including contrast enhancement, noise reduction, and cropping to focus on the meter's reading area.

4. Data Validation: Recognized values are checked against expected ranges or historical data to identify anomalies such as sudden spikes in usage.

5. Transmission: Processed data is transmitted securely to the mobile application via Wi-Fi or Bluetooth, ensuring real-time updates for the users.

6. Standby Mode: Once the reading is complete, the device reverts to low-power standby mode to conserve energy until the subsequent scheduled activation

4. Development and testing of mobile application and user interface

Development of a mobile application and user interface for automated meter reading systems. The proposed mobile application is a critical interface between end-users and a universal automated meter-reading device, emphasizing usability and intuitive operation. The application's architecture focuses on secure user authentication and efficient device management, facilitating rapid setup and seamless control.

User Authentication and Account Security.

To ensure both security and a personalized user experience, the application integrates a robust user registration and authentication system. New users create an account by providing essential details, such as a valid email and a password, enabling the secure association of user data and device configurations with individual accounts. Upon returning, users log in to access their personalized dashboard, manage devices, and monitor meter readings, maintaining a secure and streamlined experience.

Device Integration and Connectivity.

The application simplifies the onboarding of new devices. Users can add devices through an intuitive “Add Device” function, with connectivity options including Bluetooth and Wi-Fi. Guided instructions assist users in pairing devices, establishing a connection efficiently, and enabling immediate monitoring. This user-centric process minimizes technical complexity, ensuring accessible setup and reliable connectivity.

Device Management Interface.

Following successful device pairing, the application presents users with a management interface for real-time control. This interface includes options for basic settings adjustments and initiating meter readings, emphasizing clarity and ease of use. Users can activate, deactivate, and check device status and initiate updates, supporting continuous monitoring with minimal user effort.

This optimized design prioritizes accessibility and efficiency, allowing users to concentrate on managing utility consumption with minimal setup and operational demands.

Application testing. To ensure the reliability and robustness of the mobile application, a comprehensive testing strategy was implemented, encompassing functional, usability, and performance evaluations across Android and iOS platforms. Initial functional testing validated core features, including user registration, device connectivity, and data retrieval accuracy, ensuring each function met specified requirements.

Usability testing was conducted with a focus group of target users to assess the interface's intuitiveness and streamline workflows, particularly in device pairing and meter-reading functions. To evaluate the app’s responsiveness and stability, performance testing examined its behavior under various conditions, including network strengths and data loads. Cross-platform testing on Android and iOS devices also ensured uniform functionality and interface behavior, leveraging Kotlin.

Multiplatform’s capabilities for consistent operation across platforms. This rigorous testing process reinforced the application's reliability and capacity to deliver a seamless, user-centered experience aligned with the demands of an automated utility management environment.

Why did we choose the ESP-32 cam itself for our device? For the development of our device, we considered several microcontroller options that meet the key requirements: camera support and energy efficiency. The leading candidate was the ESP32 board, but we also compared it with other popular solutions: Raspberry Pi Zero W, Arduino MKR1000, and STM32F746G Discovery.

Table 1. Comparison of output data properties of expert systems and neural networks

Characteristics	ESP32	Raspberry Pi Zero W	STM32F746G Discovery
Camera	Built-in support	Additional module	Possible with an adapter
Energy efficiency	High, up to 1.67 mAh	Medium (up to 100 mAh)	HLow (up to 200 mAh)
Price	low	medium	High
Processor	Dual-core, 240 MHz	Single core, 1 GHz	Single-core, 216 MHz
Memory	520 KB of RAM	512 MB of RAM	320 KB of RAM

Review of Boards.

1. ESP32. The ESP32 is a microcontroller with a dual-core processor (240 MHz), built-in Wi-Fi and Bluetooth modules, and support for external cameras via the ESP32-CAM module. The ESP32 has become a popular choice for IoT projects thanks to its high energy efficiency and affordability.

Advantages: built-in camera support; deep sleep modes that significantly reduce power consumption (down to 1.67 mAh in our test); low cost; support for various peripheral devices;
Disadvantages: limited RAM (520 KB); specialized module (ESP32-CAM) is required for camera operation.

Suitability: Ideal for budget-constrained projects requiring autonomy and camera functionality.

2. Raspberry Pi Zero W. The Raspberry Pi Zero W is a compact single-board computer with a 1 GHz processor and built-in Wi-Fi and Bluetooth modules. It is well-suited for projects requiring greater computational power and flexibility.

Advantages: supports camera connection via the dedicated Raspberry Pi Camera module; significant memory capacity (512 MB RAM); large user community and extensive software availability; Disadvantages: high power consumption even in idle mode (up to 100 mAh); requires an additional module for camera operation, increasing costs; relatively higher cost compared to ESP324.

Suitability: best suited for projects where performance and the need for a Linux environment are critical, but energy efficiency is not a priority.

3. STM32F746G Discovery is a powerful board based on the STM32 microcontroller with a 216 MHz processor, used in projects with high computational requirements. The board supports camera connections via adapters.

Advantages: powerful processor; large RAM capacity (320 KB RAM); ability to connect cameras through external adapters.

Disadvantages: low energy efficiency (power consumption up to 200 mAh); very high cost; complexity in use due to a multi-component design.

Suitability: Suitable for high-tech projects where computational power is critical but autonomy is not.

By choosing the ESP32, we achieved the optimal balance between functionality, energy

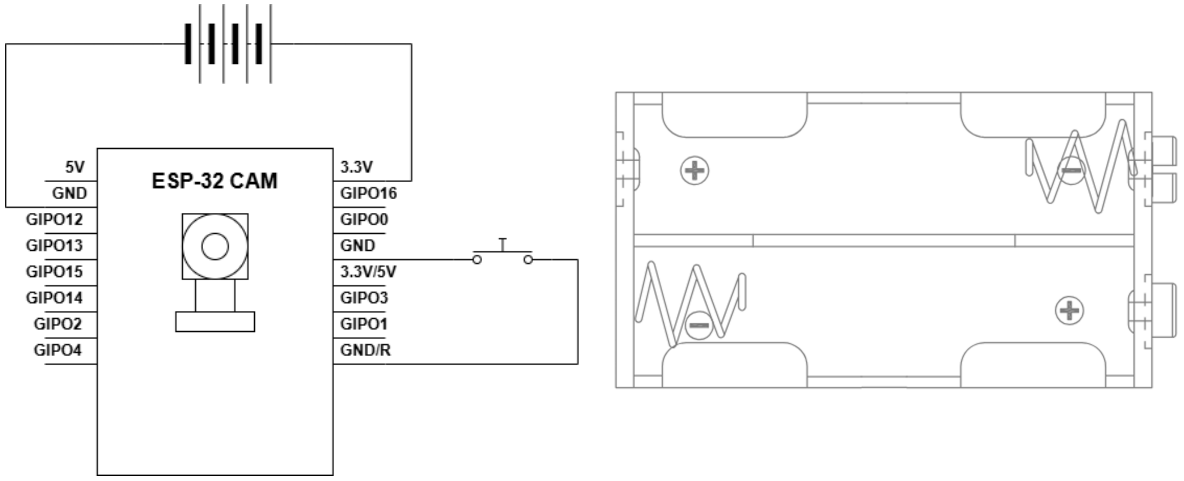
efficiency, and cost. Its support for cameras and low power consumption enables the creation of autonomous devices that can operate for extended periods without battery replacement. Additionally, the built-in Wi-Fi and Bluetooth modules provide seamless integration into IoT infrastructure, while its affordable price makes this board the perfect choice for budget-friendly projects.

5. Analysis and Optimization of Device Operational Duration

A key aspect of our device is its extended operating time, which is crucial for such solutions. We approached this issue with utmost seriousness.

First, we analyzed our competitors to determine how long similar devices could function without battery replacement. The analysis revealed that, on average, competitor devices can operate for a year. Using this information, we initiated tests to evaluate the operational duration of our device under various modes using our firmware.

Initially, we tested the device with non-optimized firmware, configured to operate in a deep sleep mode and activate once a month to read meter indicators and transmit them to utility services. For power, we chose two batteries with a capacity of 2500 mAh each. This option was selected due to the convenience of replacing batteries when necessary (Fig. 1).



a) board
a) плата

b) battery holder
б) плейсхолдер для батареї

Fig. 1 - The device resources

Testing revealed that this setup, combined with the standard plug-in for our ESP32-CAM board, was suboptimal. The batteries were discharged by 60%(1) after one month. Calculations indicated that our board consumed 4.16 mAh in this mode, resulting in an operational duration of only 50 days:

Calculation: 60% = 3000 mAh; 3000 / 30 ≈ 100 mA/day; 100 / (24) = 4.16 mAh

To determine how many days the device can operate at full charge (100%). 1. Total battery capacity: 100% = 5000 (two batteries, each with 2500 mAh). 2. Daily consumption is based on the calculations: 100 mAh/day. 3. Operational duration on a full charge: 5000 mAh / 100 mAh / day = 50 days; (5000 mAh) / (100 mAh) = 50 days.

Conclusion: The device can operate for 50 days on a full charge.

This performance was unsatisfactory and not competitive in the market. Faced with this result,

we decided to make significant changes. Several options were considered, including optimizing the firmware or increasing the batteries to four. However, adding more batteries was not appealing due to the increased cost and the inconvenience of replacing four batteries every few months. Ultimately, we opted to focus on firmware optimization.

After optimizing the firmware, we repeated the tests with the same two 2500 mAh batteries. After one month, we were pleasantly surprised by the results: the batteries were discharged by only 24%. This meant our device could now operate for approximately four months. Calculations confirmed that the board's consumption had decreased from 4.16 mAh to 1.67 mAh.

Calculation:

Step 1: Battery usage after one month. Total battery capacity: 5000 mAh (two batteries of 2500 mAh. Discharge after one month: 24%. Consumed capacity in one month = 5000 mAh × 0.24 = = 1200 mAh.

Step 2: Daily consumption. Number of days in one month: 30 days. Daily consumption = 1200 mAh / 30 days = 40 mAh/day. Hourly Consumption: 40 mAh / day / 24 hours ≈ 1.67 mAh/hour.

Step 3: Operational duration for 100% charge. Total capacity: 5000 mAh. Daily consumption: 40 mAh. Operational duration = 5000 mAh / 40 mAh/day = 125 days.

Step 4: Verify consumption rate decrease. Previously, consumption was 4.16 mAh/hour, now 1.67 mAh/hour. The device can operate at full charge for approximately 125 days (about 4 months). This improvement was a significant step forward, and we decided to retain the optimized firmware due to its enhanced energy efficiency.

However, despite these advancements, we have not yet achieved the one-year operational benchmark set by our competitors. To reach this goal, further improvements are necessary. Our plans include developing a custom board tailored to our device's needs rather than relying on the standard ESP32-CAM board. This step is expected to significantly enhance the device's energy efficiency, as competitors typically use custom-designed boards for their solutions.

6. Conclusions

This study presented a novel automated meter reading solution designed to overcome traditional challenges faced in manual data collection. Initial analysis identified critical issues, including inconsistent manual readings, difficulty accessing meters, human error in data transcription, and the limited universality of existing devices. The proposed universal solution, built around the ESP32-CAM microcontroller, effectively addressed these limitations by enabling the automated collection and wireless transmission of readings for gas, water, and electricity meters through a user-friendly mobile application.

One of the critical aspects of the proposed device was ensuring energy efficiency. Initial tests with standard firmware configurations revealed suboptimal battery performance, lasting approximately 50 days on a single charge. Recognizing this issue, significant firmware optimizations were implemented, resulting in a dramatic improvement in energy efficiency. Subsequent testing demonstrated that the optimized system significantly reduced power consumption from 4.16 mAh/hour to 1.67 mAh/hour, extending the operational duration to approximately four months on two 2500 mAh batteries.

Despite these substantial improvements, the achieved battery life still fell short of the one-year benchmark set by market competitors. As a result, the research identified the need for further enhancements through custom hardware development. Developing a custom circuit board optimized for system needs was identified as a crucial move to boost lifespan and energy efficiency for better market performance.

The developed mobile application provided secure, intuitive device management, data

visualization, and user authentication, leveraging Kotlin Multiplatform to ensure consistent performance across Android and iOS devices. Comprehensive usability and performance tests validated the application's ease of use, responsiveness, and reliability, confirming its suitability for widespread adoption.

In conclusion, this project significantly contributes to modernizing utility management systems by automating meter readings, enhancing accuracy, reducing human error, and improving consumer convenience. Although there remains room for improvement in hardware optimization, the developed solution successfully meets core objectives, establishing a solid foundation for future development and scalability within automated utility management technologies.

Conflicts of Interest: the authors declare no conflict of interest.

References

1. Das, M., Kaur, A., Sadiq, S., Ekka, G.S., Ghosh, T.K. (2024). Hybrid home automation system using IoT. *In Advances in Networks, Intelligence and Computing*, pp.198-209. CRC Press ISBN 9781003430421
2. Zubkov, O.V., Yakovenko, O.C., Starokozev, C.V., Skorbatuk, M.V. (2024). Development and research of an algorithm for automated recognition of gas meter readings. *Radiotekhnika*, (219) , 46-52 [in Ukrainian] DOI: https://doi.org/10.30837/rt.2024.4.219.05
3. Labunsky, V., Zaschepkina, N., Labunskaya, A. (2023). Improving the method of water meter calibration. Measuring and computing devices in technological processes, (2), 67-71. [in Ukrainian]. DOI: https://doi.org/10.31891/2219-9365-2023-74-22
4. AlRuwais, S., AlQahtani, R., AlHajri, N., AlHashim, B., Bashar, A., & AlZubaidi, L. (2021). S-LIGHT: Smart LED Lamppost using PWM-based Adaptive Light Controller. *In 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 325-331). IEEE. DOI: https://doi.org/10.1109/CSNT51715.2021.9509652
5. Navarrete-Sanchez, M. A., Olivera-Reyna, R., Olivera-Reyna, R., Perez-Chimal, R. J., & Munoz-Minjares, J. U. (2025). IoT-Based Classroom Temperature Monitoring and Missing Data Prediction Using Raspberry Pi and ESP32. *Journal of Robotics and Control (JRC)*, 6(1), 234-245 DOI: https://doi.org/10.18196/jrc.v6i1.24345
6. Abadade, Y., Temouden, A., Bamoumen, H., Benamar, N., Chtouki, Y., & Hafid, A. S. (2023). A comprehensive survey on tinyml. IEEE Access, 11, 96892-96922. DOI: https://doi.org/10.1109/ACCESS.2023.3294111
7. Kaur, A., Jadli, A., Sadhu, A., Goyal, S., & Mehra, A. (2021). Cloud based surveillance using ESP32 CAM. In 2021 international conference on intelligent technology, system and service for internet of everything (ITSS-IoE) (pp. 1-5). IEEE. DOI: https://doi.org/10.1109/ITSS-IoE53029.2021.9615334
8. Kumar, S., Sharma, K., Raj, G., Datta, D., Ghosh, A. (2022). Arduino and ESP32-CAM-Based Automatic Touchless Attendance System. In: Sikdar, B., Prasad Maity, S., Samanta, J., Roy, A. (eds) *Proceedings of the 3rd International Conference on Communication, Devices and Computing. ICCDC 2021. Lecture Notes in Electrical Engineering, vol 851.* Springer, Singapore. DOI https://doi.org/10.1007/978-981-16-9154-6_14
9. R. R. PBV, V. Sonaleo Mandapati, S. L. Pilli, P. Lahari Manojna, T. H. Chandana and V. Hemalatha, "Home Security with IOT and ESP32 Cam - AI Thinker Module," 2024 *International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS)*, Coimbatore, India, 2024, pp. 710-714, DOI: https://doi.org/10.1109/ICC-ROBINS60238.2024.10533960

РОЗРОБКА УНІВЕРСАЛЬНОЇ ЕНЕРГОЕФЕКТИВНОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ ЗНЯТТЯ ПОКАЗАНЬ ЛІЧИЛЬНИКІВ З ВИКОРИСТАННЯМ ESP32-CAM

Тетяна Коробейнікова[1], кандидат технічних наук, доцент,
e-mail: tetiana.i.korobeinikova@lpnu.ua, ORCID: https://orcid.org/0000-0003-2487-8742
Олександр Ремінний[1], кандидат технічних наук, асистент, e-mail: sasha.reminnyi@gmail.com,
ORCID: https://orcid.org/0009-0005-5119-3695
Роман Байтала[1], студент кафедри комп'ютеризованих систем автоматики,
e-mail: roman.baitala.ir.2023@lpnu.ua
Владислав Кирик[1], студент кафедри комп'ютеризованих систем автоматики,
e-mail: vladyslav.kyryk.ir.2023@lpnu.ua
Данило Стецький[1], студент кафедри комп'ютеризованих систем автоматики,
e-mail: danylo.stetskyi.ir.2023@lpnu.ua
[1]*Національний університет «Львівська політехніка»,*
вул.С.Бандери, 12, Львів, 79000, Україна
Рукопис надійшов 21 квітня 2025 р. Отримано після рецензування 22 травня 2025 р.
Прийнято 22 червня 2025 р.

Анотація: У цій статті обговорюється проектування та розробка універсальної автоматизованої системи зняття показань лічильників, здатної працювати з різними типами ресурсів, включаючи воду, газ та електроенергію. Розроблена система вирішує загальні проблеми, пов'язані з ручним зняттям показань лічильників, такі як доступність, непослідовність запису даних та людські помилки. Основною інновацією є інтеграція модуля ESP32-CAM для автоматизації захоплення зображень та передачі даних до комунальних служб через зручний мобільний додаток. Особливий акцент зроблено на оптимізації енергоефективності для забезпечення тривалої автономності пристрою. Запропонована система включає надійний алгоритм попередньої обробки зображень, перевірку показань лічильників та безпечний бездротовий зв'язок. Ретельне тестування на платформах Android та iOS продемонструвало зручність, функціональність та стабільну роботу програми. Зусилля з оптимізації значно збільшили час роботи пристрою від батареї з приблизно 50 днів до чотирьох місяців. Пропонується подальше вдосконалення, зокрема розробка спеціальної апаратної плати для досягнення стандартної тривалості роботи в один рік.

Ключові слова: *автоматизоване зчитування лічильників, ESP32-CAM, IoT, мобільний додаток, енергоефективність, нейронна мережа, управління комунальними послугами*

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 1 (27)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 1 (27)

DOI: https://doi.org/10.26565/2519-2310-2025-1-04
УДК 004.056.55:004.932

МОДЕЛЮВАННЯ І ОЦІНКА ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ОСНОВНИХ ПРОЦЕДУР, ПОЧАТКОВИХ ЕТАПІВ ГІБРИДНОГО СТЕГАНОАЛГОРИТМУ

Микита Гончаров[1], аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, e-mail: m.honcharov@student.karazin.ua, ORCID: https://orcid.org/0000-0002-9790-7260
Сергій Малахов[1], к.т.н., ст. науковий співробітник, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, e-mail: malakhov@karazin.ua, ORCID: https://orcid.org/0000-0001-8826-1616
[1]*Харківський національний університет імені В.Н. Каразіна, 61022, проспект Свободи, 4, Харків, Україна*

Рукопис надійшов 1 березня 2025 р. Отримано після рецензування 1 квітня 2025 р. Прийнято 2 травня 2025 р.

Анотація: У сучасних умовах зростання кіберзагроз стеганографія відіграє ключову роль у забезпеченні конфіденційності даних, приховуючи їх у масивах цифрових даних (зображення, звук, файлові системи тощо). На відміну від криптографії, стеганографія приховує сам факт передачі інформації, що робить її незамінною для захисту даних в інформаційно-комунікаційних системах з обмеженими ресурсами. Необхідність створення енергоефективних і адаптивних алгоритмів, які поєднують стійкість контенту, високу якість контейнера та низьку обчислювальну складність, підкреслює актуальність проведених досліджень. У роботі проведена оцінка обчислювальної складності процедур попередньої обробки вхідних даних та визначено їх вплив на ефективність подальшої інкапсуляції даних. В якості основи для моделювання обрано один із можливих варіантів згладжування малоінформативних областей вихідних зображень. Виконано оцінку: - продуктивності за часом виконання для різних типів зображень; показником *PSNR*; ймовірності кольорового перепаду яскравості та кількістю сформованих опорних блоків (ОБ) зображень. В ході моделюванні досліджено наслідки згладжування текстур вихідних зображень в умовах варіювання розміру матриць згладжування та значення різниці яскравості пікселів. Зроблено підрахунок базових операцій (арифметичних, логічних, порівнянь) для кожного блоку та визначена загальна складність відповідних етапів алгоритму. Експериментальна оцінка проводилася шляхом вимірювання часу виконання процедур, оцінці якості зображень за метрикою *PSNR*, розрахунком ймовірності перепаду яскравості та підрахунком кількості сформованих серій ОБ. Для оцінки ефективності досліджуваних процедур, використані тестові зображення із різними текстурними характеристиками. Отримані результати підтвердили, що етап попереднього згладжування покращує вихідні умови для формування серій ОБ (порівняно з їх відсутністю). Впровадження етапу згладжування забезпечує зменшення шуму у малоінформативних областях, що сприяє підвищенню однорідності блоків та розширює діапазон комбінаторики наявних параметрів кодування (як спосіб протидії спробам неавторизованого вилучення контенту). Гнучке налаштування розміру блоку та значень порогу загрублення яскравості елементів зображень, дозволяє забезпечити адаптацію процесу згладжування до різних типів зображень та поточних ресурсних обмежень використовуваних апаратних платформ. Запропонований підхід

до попередньої обробки даних, створює потрібні умови для формування серій ОБ, покращує стійкість контенту та підтримує низькій рівень візуальних спотворень. Адаптивне налаштування параметрів згладжування дозволяє ефективно використовувати алгоритм на платформах з обмеженими ресурсами. Це робить його перспективним для застосування в складі мобільних додатків. Отримані результати сприяють подальшому удосконаленню стеганографічних методів захисту інформації та відкривають нові перспективи для подальших досліджень.

Ключові слова: *інформаційна безпека, загрози, кібератака, обчислювальна складність, інкапсуляція даних, несанкціонований доступ, стеганографія, кодування довжин серій*

Як цитувати: Гончаров М., Малахов С., Моделювання і оцінка обчислювальної складності основних процедур, початкових етапів гібридного стеганоалгоритму. *Комп’ютерні науки та кібербезпека*. 2025; № 1(27): С. 41–59. https://doi.org/10.26565/2519-2310-2025-1-04

In cites: Honcharov M., Malakhov S. (2025). Modeling and evaluation of the computational complexity of the main procedures, the initial stages of the hybrid steganographic algorithm. *Computer Science and Cybersecurity.* 1(27): 41–59. https://doi.org/ 10.26565/2519- 2310-2025-1-04 (in Ukrainian)

1. Вступ

Сучасні цифрові технології забезпечують широкі можливості для обміну, обробки і зберігання інформації, зумовлюючи нові перспективи в галузі розвитку інформаційно-комунікаційних технологій [1-2]. Поряд з цим, розвиток інформаційних технологій (ІТ) неминуче створює передумови для появи нових загроз інформаційної безпеки (ІБ), таких як несанкціонований доступ, перехопленням і фальсифікація даних та багато ін. Це зумовлює потребу в постійному вдосконаленні та розробці нових технологій і методів парирування сучасних загроз [3-4]. У цьому контексті стеганографія є важливим інструментом для приховування потрібної інформації у цифрових носіях – переносниках даних різного типу, дозволяючи зберігати конфіденційність прихованого каналу передачі даних без привернення уваги до факту його існування [1,5]. Це забезпечує непомітну передачу конфіденційних даних, роблячи стеганографію важливою складовою в загальному спектрі відомих інструментів безпеки. Розробка стеганографічних методів, що одночасно поєднують високі скритність функціонування і стійкість до спроб «злому» потайного контенту, та мають високі обчислювальну ефективність й адаптивність до різних апаратних платформ, є актуальним завданням. Ключовим питанням у зазначеній композиції факторів й умов, є досягнення балансу між збереженням характерних статистичних властивостей використовуваного контейнера – переносника даних та мінімальним рівнем його демаскуючих спотворень в умовах впливу стохастичних ресурсних обмежень (наприклад, поточна загрузка CPU, залишковий заряд акумуляторної батареї гаджету, обмеження на використовувану смугу частот і т.і.) [1,5,8].

Практичне застосування стеганографії охоплює широкий спектр сценаріїв: від захисту конфіденційної інформації в корпоративних ІКС до забезпечення безпеки даних у мобільних пристроях [2,6,9]. Сучасні методи стегановставки повинні одночасно враховувати, як статистичні характеристики використовуваних цифрових носіїв, так і особливості людської зорової системи, щоб забезпечити непомітність змін у контейнері [1,5,7-8]. Також, з огляду на різноманітність апаратних платформ, від потужних стаціонарних серверів до персональних

мобільних пристроїв, використовувані методи інкапсуляції даних, повинні бути гнучкими та оптимізованими для роботи в умовах обмежених обчислювальних ресурсів [7]. В цьому сенсі, особлива увага приділяється розробці методів й технік, які дозволяють оперативно й ефективно суміщати властивості цифрових контейнерів і контенту, мінімізуючи ризик виявлення факту стегановставки статистичними та/чи візуальними (*в межах даної роботи*) методами аналізу [5,7]. Відповідно, матеріали цієї роботи мають на меті подальше вдосконалення окремих процедур обробки вихідних даних зображень контейнеру і контенту, шляхом аналізу й оптимізації ключових етапів обробки даних, що в підсумку сприятиме підвищенню їхньої практичної застосовності та покращенню адаптивність алгоритму до різних станів комбінаторики зовнішніх факторів, і статистичних властивостей, безпосередньо об'єктів обробки (*в даному разі напівтонових зображень*) [3-4].

2. Структура тестового алгоритму та призначення функціональних модулів

В ході досліджень проведено моделювання 3-х варіантів згладжування малоінформативних ділянок вихідних тестових зображень, з можливістю зміни допустимого значення різниці яскравості сусідніх пікселів (P_Z) та розміру матриць згладжування зображень, на задану фіксовану величину [4]. Основною метою попередньої підготовки вихідних даних є, перетворення структури вхідних зображень для зменшення загальної обчислювальної складності алгоритму обробки та створення потрібних умов для подальшого ускладнення аналізу й неавторизованої екстракції прихованого контенту [3]. Ця підготовка (*далі передобробка*) передбачає зменшення кількості візуально непомітних перепадів яскравості елементів зображень, тобто проведення процедури фонового згладжування малоінформативних областей вихідних зображень. Досліджені варіанти передобробки забезпечують необхідні початкові умови для покращення процесу інкапсуляції даних, інтенсифікуючи процес формування серій опорних блоків (ОБ) та розширюючи потенційну комбінаторику мультиплексування поточних параметрів сформованого масиву серій ОБ [4]. Коротко розглянемо основні відмінності, щодо особливостей оцінки обчислювальної складності процедур, які притаманні для кожного із модельованих варіантів передобробки.

Оцінку обчислювальної складності модельованих варіантів передобробки вихідних зображень, виконано спираючись на аналіз кількості базових операцій, потрібних при обробці кожного вихідного блока та, відповідно, загальної кількості цих блоків. Умовно будемо вважати, що, вихідне зображення має розмір $M \times M$ ел, а розмір субблоків при його сегментації для подальшої обробки, становить $N \times N$ елементів. Т.ч., результуюча кількість субблоків, що утворюються в результаті фрагментації вихідного кадру тестового зображення, складає приблизно $(M/N)^2$, а загальна процедурна складність алгоритму визначається, як добуток кількості блоків, на кількість виконуваних операцій для кожного окремого субблоку. Так, якщо обробка одного блока потребує $O(N^2)$ операцій (*де «О» це асимптотична оцінка складності алгоритму, що описує верхню межу кількості операцій*), результуюча складність для вихідного зображення становитиме $O(M^2)$. Слід мати на увазі, що фактична продуктивність залежить не лише від асимптотичної складності, а і від певних незмінних чинників, типу виконуваних операцій та особливостей використовуваної апаратної платформи.

Важливо розуміти, що розмірність обраного блоку матриці згладжування «N», є ключовим параметром, який самим безпосереднім чином впливає на результати проведеного згладжування вихідного фрагменту зображення, та ефективність подальшого використання методу кодування довжин серій. Так, малий розмір блоків (N = 3÷5 ел.) забезпечує високу швидкість, але враховує локальний розподіл яскравості елементів, а занадто великий розмір блока (*наприклад, $N \geq 7$ ел.*) збільшує обчислювальні витрати, та потребує додаткових заходів

(підходів) для врахування відомостей про появу/початок лінії контурів, зберігаючи т.ч. важливу інформацію та зменшуючи наслідки утворення нетипових артефактів. В цілому, змінюючи розмірність матриці згладжування, можна забезпечити необхідний компроміс між допустимим ступенем спотворень контейнера переносника даних та одержуваної обчислювальною складністю. Т.ч., вибір потрібного значення «N», залежить від конкретного завдання, типу використовуваних зображень (*у зв'язці пари «контейнер–контент»*), розміру «M» та доступних - вільних обчислювальних і енергетичних ресурсів використовуваної апаратної платформи (*RAM, CPU, залишкова ємність АБ і т.і.*). Тому оперативний та обчислювально щадний аналіз складності структури вихідних масивів даних, має базуватися на механізмах, котрі пройшли ретельну експериментальну апробацію [1,5,8].

Лабораторний варіант. Цей варіант обробки не передбачає ніякої передобробки і використовується лише для порівняння результатів моделювання інших варіантів: - за результативністю та параметрами формування масиву серій ОБ; - обчислювальною складністю; - отримуваним співвідношенням масивів серій ОБ у пов'язаній системі «контент-контейнер», котра впливає на параметри комбінаторики, безпосередньо на етапі стеганографічної вставки даних. Тобто, в даному випадку, вихідне зображення розбивається на блоки заданого розміру $N \times N$ ел, без будь-якої зміни значень яскравості пікселів, а всі наступні етапи алгоритму використовують вихідне зображення, як воно є. Відповідно, обчислювальна складність цього варіанту становить $O(M^2)$, що відповідає операціям читання зображення та його розбиття на блоки встановленого розміру, тобто з точки зору залучення обчислювальних ресурсів, цій варіант є умовно «найбільш ресурсомістким». Вочевидь, що відсутність будь-якої попередньої обробки, звужує умови для більш ефективного формування серій ОБ и таким чином обмежує диспаритет ОБ зображень в системі «контент - контейнер» та потенційну комбінаторику ОБ на етапі мультиплексування ОБ контенту (*як механізму з протидії спробам несанкціонованого вилучення контенту*).

Перший варіант. Вихідне зображення фрагментується на квадратні блоки N×N ел, що відповідає будь-якому непарному значенню (3×3, 5×5 і т. ін). Для кожного блоку оцінюється різниця між яскравістю його центрального елементу та яскравістю його периферійних пікселів. В разі, якщо ця різниця менша за встановлену порогову величину (P_Z), значення яскравості відповідного периферійного елемента змінюється на значення яскравості його центрального пікселю. Якщо ж ця різниця перевищує встановлене P_Z, то значення периферійного елементу залишається без змін. Таким чином, згладжування кожного наступного блоку здійснюється шляхом послідовного порівняння та зміни поточних значень периферійних пікселів, відносно вихідного значення центрального елементу. В цьому разі, обчислювальна складність обробки одного блоку, складає $O(N^2)$, оскільки для кожного блоку виконується (N^2 - 1) порівнянь між центральним та периферійними елементами. Загальна кількість блоків у зображенні розміром M×M дорівнює $(M/N)^2$. Т.ч., результуюча обчислювальна складність розраховується, як $O(M^2/N^2) \times O(N^2)$, що спрощується до $O(M^2)$. В даному випадку, операції заміни значень пікселів не впливають на асимптотичну складність, оскільки вони виконуються в межах обробки блоку за $O(N^2)$. Цей варіант є прийнятним з точки зору ресурсних витрат, оскільки залежність від наслідків збільшення розміру блоку (*матриці згладжування*), нівелюється при обробці всього масиву зображення. В цілому, для зображень зі значними зі значним розкидом яскравості складових елементів, цей варіант може виявитись менш ефективним, оскільки згладжування базується лише на відомостях про стан центрального пікселю, що не завжди відображає загальні структурні властивості блоку, особливо при збільшенні його розмірів (*більше 5×5 ел.*).

Другий варіант. Вихідне зображення поділяється на субблоки розміром $N \times N$ (*де «N» відповідає будь-якому непарному значенню*), після чого для кожного окремого блоку оцінюється різниця між яскравістю його центрального елементу та яскравістю всіх інших пікселів. В разі,

якщо отримана різниця перевищує встановлений поріг загрублення - P_Z, то всі такі елементи блоку, замінюються на середнє значення яскравості всіх елементів даного блоку (*тобто, не значенням амплітуди центрального пікселю, як у 1-му варіанті*). Якщо жодна отримана різниця не перевищує заданий поріг «P_Z», то все залишається як є. Іншими словами, згладжування яскравості здійснюється шляхом заміни всіх значень елементів, що відрізняються від центрального пікселю більш ніж на величину «P_Z», на нове значення, що відповідає середньому значенню усіх елементів блоку. Обчислювальна складність обробки кожного блоку становить $O(N^2)$, оскільки виконується (N^2 - 1) порівнянь між центральним пікселем і його периферійними елементами. В разі заміни амплітуди на нове значення, обчислюється середнє значення всіх N^2 елементів, що також вимагає $O(M^2)$ операцій. Загальна кількість субблоків у зображенні розміром M×M дорівнює $(M/N)^2$. Т.ч., сумарна обчислювальна складність 2-го варіанту визначається, як $O(M^2/N^2)\times O(N^2)$, що спрощується до $O(M^2)$. Операції обчислення середнього значення не впливають на асимптотичну складність, оскільки вони виконуються в межах обробки блоку за $O(N^2)$. Хоча асимптотична складність другого й першого варіантів збігається, однак реальний час виконання може бути дещо більшим через додаткові операції обчислення середнього значення (*для всіх субблоків*). В цілому, порівняно з першим варіантом, другий варіант згладжування є більш ефективнішим (*з точки зору формування потрібних стартових умов для виконання кодування методом серій*), оскільки заміна на середнє значення враховує всі пікселі блоку, що забезпечує підтримку/формування більш однорідних ділянок зображення. Однак обчислення середнього значення яскравості всіх субблоків, додає витрати, які можуть бути помітними в разі використання великих субблоків (*наприклад, більш ніж 11×11 ел.*), чи великих розмірах вихідного зображення та/чи на пристроях із низькою продуктивністю.

Третій варіант. Вихідне зображення поділяється на субблоки потрібного розміру $N\times N$. Після цього для кожного субблоку обчислюється різниця між яскравістю всіх можливих пар пікселів, що відповідає попарному порівнянню N^2 елементів. В разі, якщо хоча б одна пара пікселів дала різницю, що перевищує заданий поріг загрублення «P_Z», то цей блок залишається без змін (*як спосіб збереження можливого контуру*). У випадку, якщо жодне порівняння не перевищує поріг «P_Z», усі значення пікселів змінюються на середнє значення яскравості. Обчислювальна складність обробки одного блоку становить $O(N^4)$, оскільки виконується попарне порівняння всіх N^2 ел., а кількість таких пар дорівнює $C(N^2, 2) = N^2 (N^2 - 1) / 2$. У разі заміни вихідних значень, обчислення середнього значення всіх N^2 елементів, потребує $O(N^2)$ операцій, але ця складність є менш значущою порівняно з $O(N^4)$. Загальна кількість блоків у зображенні розміром $M\times M$ дорівнює $(M/N)^2$. Т.ч., складність цього варіанту обчислюється, як $O(M^2/N^2)\times O(N^4)$, що спрощується до $O(M^2 \times N^2)$. Ця складність вказує на квадратичну залежність, як від розміру вихідного зображення, так і від розміру субблоків, що робить цей варіант непрактичним для великих субблоків, великих зображень та систем з обмеженою обчислювальною потужністю.

Так, наприклад, для вихідного зображення розміром 1050×1050 піх (M = 1050) та субблоків 7×7 ел. (N = 7), загальна складність складає $1050^2\times 7^2 \approx 54$ млн. операцій. А для субблоків розміром *3×3* ел., вона вже становитиме $1050^2\times 3^2 \approx 9$ млн. операцій, що є меншою порівняно з N = 7, та перевищує складність інших варіантів. При цьому, цей варіант забезпечує більш ретельний аналіз структури зображення, що може бути корисним для випадків, де зображення не рясніє частими переходами яскравості сусідніх елементів і створює для стеганоаналітика комфортні умови для візуальної локалізації (виявлення) можливих змін початкового стану окремих елементів або ділянок. Однак, порівняно висока обчислювальна складність робить цей варіант непрактичним для більшості випадків застосувань при умові великих значень *M* чи *N*, що декілька знецінює його практичне використання в реальних сценаріях, особливо на пристроях з обмеженою потужністю або в умовах дефіциту ресурсів.

3. Оцінка обчислювальної складності процедур передобробки вихідних даних

Результати експериментальної оцінки обчислювальної складності реалізованих процедур, розглянемо на прикладі 2-го варіанту передобробки, як найбільш збалансованого з точки зору наслідків згладжування. В межах моделювання досліджувалися часові характеристики роботи тестового алгоритму, вплив розмірності використовуваних субблоків і параметрів згладжування (P_Z) на якість відтворення зображення, яка оцінювалась за показником *PSNR* (*пікового значення С/Ш*). Окремо проведено розрахунок кількості сформованих ОБ та ймовірності перепаду яскравості для декількох типів тестових зображень й їх перетворених копій, отриманих після процедур передобробки за вар. №2, та наведено оцінку обчислювальної складності цього варіанту для обраних зразків зображень. В якості тестових зображень були обрані характерні зображення 3-х різних типів (Мнемосхема, Пейзаж і Пейзаж (*два останні в варіанті «Комп’ютерна графіка», тобто CG*)), що відрізняються значеннями ймовірності перепаду яскравості [10] між сусідніми пікселями (*див. рис. 1*). Використання характеристики ймовірності перепаду яскравості між сусідніми елементами, дозволяє визначити загальний рівень текстурної складності вихідних зображень для наступного застосування до них, найбільш збалансованих параметрів згладжування. Також, на рис.1 наведено відповідну схему розгортки (*тобто, вибірки елементів для реалізації тих чи інших процедур обробки (у даному випадку, оцінки ймовірності перепаду яскравості)*), яка використовувалася в межах даного циклу тестових випробувань. Важливо підкреслити, що діюча схема розгортки є одним із ключових параметрів, якій забезпечує послідовне виконання 2-х різних функцій: - на етапі предобробки визначає послідовність обходу й аналізу вихідних даних, а на етапі формування масиву довжин серій ОБ, забезпечує стійкість контенту до спроб його неавторизованого вилучення [11-13], так як тільки легітимним користувачам відома її діюча схема. Вочевидь, що в залежності від налаштувань алгоритму схеми розгортки на етапі передобробки і формування серій ОБ можуть відрізнятися. В цілому, різні схеми організації розгортки серій ОБ відповідають різним станам відповідного елементу складеного ключа екстрактора даних [3,11]. Використання різних схем розгортки та способів вибірки діючих пар параметрів (тобто, безпосередньо сам ОБ + довжина серії) або тільки їх окремих елементів (наприклад, тільки самого ОБ), формує широке комбінаторне поле для протистояння спробам неавторизованого вилучення контенту, посилюючи роль цього елемента в структурі ключа екстрактора [3]. Т.ч., використання різних способів організації схем розгортки та вибірки її окремих складових, утворює окрему позицію (див. роботи [11-13]) в загальній структурі складеного ключа екстрактора даних [3].

В межах даної роботи на обох етапах алгоритму (*згладжування та формування серій ОБ*), було використано одну й теж схему розгортки «***По рядках***» (Рис.1(в)). Слід зауважити, що використана схема розгортки не є обчислювально складною. Водночас застосування більш складних схем розгортки значно ускладнює роботу атакуючого та підвищує загальну стійкість контенту до спроб його «злому» [14-15]. Зокрема, двопрохідні та випадкова схеми, значно посилюють візуальну фрагментацію вихідного контенту, в разі хибного підбору діючих параметрів кодування контенту. Іншими словами, в даному разі, зростає кількість формованих серій ОБ і розширюється комбінаторне поле можливих варіантів їхньої обробки. З одного боку це виглядає дуже добре, але підвищується обчислювальна складність процедур, що суперечить загальному вектору зусиль, стосовно зниження обчислювальної складності всього алгоритму в цілому [2]. Детальний аналіз цих взаємопов'язаних процесів, наведено в роботах [11-15].

Отримані в ході моделювання часові характеристики для тестових зображень різного типу (див. рис.1 *(а,б,г)*) в умовах застосування 2-го варіанту передобробки, наведено в табл. 1. У ній наведено результати виконання п’яти однократних повних циклів процедур згладжування та

обчислений середній час їх виконання [4]. Для порівняння використовувалися два варіативні параметри: - розмірність субблоків N та поріг загрублення «P_Z», що дозволяє оцінити їх вплив на обчислювальну ефективність і якість згладжування для різних типів тестових зразків.

Ймовірність перепаду яскравості/кольору пікселів є важливою характеристикою цифрових зображень, що має суттєве значення у задачах їх аналізу, класифікації та сегментації [10]. Під «перепадом» будемо розуміти зміну значення відповідного параметра (в даному разі яскравості) між сусідніми елементами зображень, згідно з вибраної схеми розгортки (тобто, послідовності вибірки потрібних значень), як це показано на рис. 1 у роботі [15]. Ця величина трактується, як імовірність випадкової події, котра відповідає переходу між діючими станами яскравості сусідніх пікселів чи блоків. Вона залежить від статистичних властивостей конкретних зображень, їх структури та застосованої шкали квантування складових елементів.

Для оцінки ймовірності перепаду яскравості до уваги береться довжина серій однакових пікселів або цілих субблоків (у межах моделювань, аналогічних до [7,16]). Це дозволяє виділити умовні ділянки з високою та низькою структурній складністю, що є принципово важливими при подальшій обробки зображень. Ймовірність перепаду яскравості, опосередковано характеризує інтенсивність переходів між різними рівнями яскравості або кольоровими відтінками сусідніх (за розгорткою) елементів. Значний перепад вказує на складне - насичене різними деталями зображення, тоді як поступові, плавні або протяжні зміни структури зображень свідчать про певну однорідність зображення й низький рівень його деталізації, що зумовлює низькі значення відповідної ймовірності.

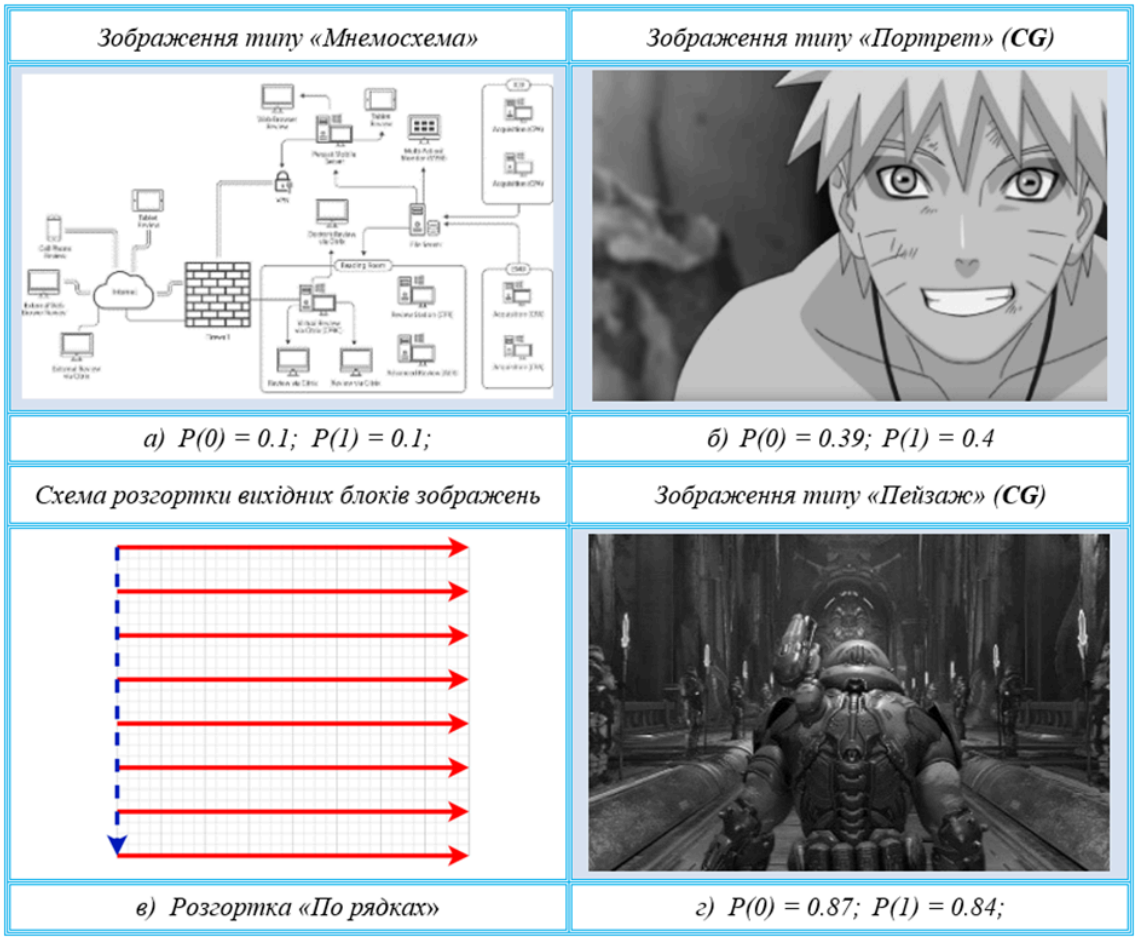


Рис. 1 – Вихідні тестові зображення (а, б, г) та використана схема розгортки (в)

Fig. 1 – Source test images (a, b, d) and the scanning scheme used (c)

Таблиця 1. Час виконання* операцій для 2-го варіанту обробки тестових зображень
Table 1. Execution time of operations in the second processing variant for different image types*

Значення порогу загрублення (Pz)	**Тип тестового зображення**					
	Мнемосхема		Портрет (*Комп. графіка* - ***CG***)		Пейзаж (*Комп. графіка* - ***CG***)	
	N = 3	***N = 7***	***N = 3***	***N = 7***	***N = 3***	***N = 7***
Pz = 3	*0.498*	*0.501*	*0.479*	*0.516*	*0.497*	*0.51*
Pz = 7	*0.501*	*0.518*	*0.477*	*0.504*	*0.491*	*0.514*
Pz = 14	*0.493*	*0.51*	*0.471*	*0.515*	*0.517*	*0.567*

** - Час виконання [с] при різних розмірностях блоків [розраховано середній час за результатами п'яти однократних повних циклів процедур згладжування]*

У межах даного циклу досліджень, оцінка ймовірності перепаду яскравості виконувалась відразу у двох просторових метриках: - ***загально*** і ***локально*** (див. рис. 1 в [10]). Перший варіант (*далі позначається, як «p(0)»*) полягає в обчисленні ймовірності для всього вихідного масиву/кадру зображення. Другий варіант (*позначається, як «p(1)»*) полягає в обчисленні ймовірності перепаду окремо для кожного із субблоків (розміром $N \times N$), на які поділено вихідне тестове зображення. Відповідно, у табл. 2 представлено порівняльні результати обчислення ймовірностей перепаду яскравості *P(0)* та *P(1)* вихідних зображень після реалізації процедур згладжування згідно з процедурами Вар.№2 (див. п.2). Розрахунки проведено для 3-х різних значень параметру порогу загрублення P_Z (3,7,14 градацій яскравості), котрі відповідають різним режимам обробки та 2-х розмірностей субблоків (3×3 та 7×7 ел.). Значення ймовірностей надано у десятковому форматі, що дозволяє якісно оцінити структуру оброблюваного ображення й класифікувати його тип.

Таблиця 2. Ймовірність перепаду яскравості після згладжування для 3-х типів зображень
Table 2. Probability of brightness difference after smoothing for 3 types of images

Поріг загрублення (Pz)	***P(0) – покадровий аналіз*** *(загальна статистика)*					
	Мнемосхема		**Портрет** *(CG)*		**Пейзаж** *(CG)*	
	N = 3	***N = 7***	***N = 3***	***N = 7***	***N = 3***	***N = 7***
Pz = 3	*0.006;*	*0.007;*	*0.029;*	*0.02;*	*0.05;*	*0.022;*
Pz = 7	*0.006;*	*0.007;*	*0.032;*	*0.025;*	*0.063;*	*0.033;*
Pz = 14	*0.007;*	*0.007;*	*0.033;*	*0.029;*	*0.073;*	*0.048;*
	P(1) – блочний аналіз *(локальна* статистика)*					
Pz = 3	*0,003;*	*0,005;*	*0,023;*	*0,016;*	*0,027;*	*0,01;*
Pz = 7	*0,003;*	*0,006;*	*0,028;*	*0,024;*	*0,045;*	*0,023;*
Pz = 14	*0,004;*	*0,006;*	*0,03;*	*0,029;*	*0,06;*	*0,04;*

** - Ймовірності отримані для тестових зображень після процедур згладжування. Ці значення дозволяють оцінити вплив згладжування на структуру зображень та ступінь їх зміни яскравості.*

Використання різних розмірностей субблоків мало на меті продемонструвати їх взаємозв'язок (*через ймовірність*) з одержуваними наслідками перетворень. Так, блоки меншої розмірності забезпечують помірне згладжування з мінімальним - щадним впливом на дрібні деталі, тоді як більші блоки демонструють інтенсифікацію процесу, що помітно знижує локальну варіативність (*див. Табл.2, стовпці N=7 для «Портрет CG» і «Пейзаж CG»*) чим зумовлює появу певних артефактів (*відносно оригіналу*) та декілька збільшує обчислювальну складність. Т.ч., застосований підхід дозволяє оцінити, яким чином розмірність субблоків й параметр «P_Z» впливають на кінцеві результати обробки, які, в свою чергу, надають можливість забезпечити компроміс між збереженням деталей, зменшенням шумів й створенням однорідних ділянок зображень (що є вкрай корисним для формування масиву серій ОБ та зменшенням обчислювальної складності загального алгоритму на наступних етапах алгоритму [4]).

При оцінці ймовірності перепаду для всього кадру (*P(0)*), спостерігається загальна тенденція на її зростання із збільшенням P_Z, незалежно від розмірності субблоків (N). При цьому, збільшення розмірностей блоків, призводить до суттєвого зменшення ймовірності перепаду яскравості (*табл.2, стовбці «Портрет CG» і «Пейзаж CG»*), тобто згладжування текстури вихідного зображення посилюється. Однак із зростанням значення «P_Z» ця тенденція помітно нівелюється. Так, наприклад: - для зображення типу *«Пейзаж CG»* при розмірностях блоків 3×3 та 7×7 ел., інтенсивність процесу згладжування уповільнюється в 1,5 рази (з 2,27 до 1,52). Причому для умов локальної статистики (*P(1)*), для таких же параметрів обробки (*N* та P_Z), відповідна різниця стає ще більшою – в 1,8 рази (*з 2,71 до 1,5; 2,71/1,5=1,81*). Крім того, слід враховувати той факт, що збільшення умовної верхньої межі загрублення параметру *«P_Z»*, в межах кожної розмірності субблоків, неминуче призводить до погіршення ефекту вирівнювання вихідної текстури через збереження набагато більшої кількості дрібних (незначних) перепадів яскравості в оброблюваних блоках. Інакше кажучи, ефект згладжування значно більшою мірою залежить від використовуваної розмірності блоків і обраного варіанту їх обробки, ніж від тенденції збільшення параметра *«P_Z»*.

У режимі блочного аналізу (тобто, P(1)) ймовірності «перепаду» для всіх типів зображень, дещо нижчі, що відповідає більш стабільним текстурам для кожного з отримуваних субблоків. Це свідчить про ефективність механізму блокової декомпозиції з усередненням перепадів яскравості складових елементів.

Відносно зображень типу ***«Мнемосхема»***, обчислення *локальної* статистики очікувано дає більш низьку ймовірність перепаду яскравості (однорідність), ніж її розрахунок для всього кадру, причому збільшення верхньої межі загрублення параметру *«P_Z»*, практично не впливає на процес згладжування, що обумовлюється специфічними особливостями структури цих зображень. В цьому сенсі, збільшення розмірностей субблоків, призводить до значно більш очевидніших результатів, причому, в даному випадку, радикально відмінним від наслідків обробки інших типів зображень (*див. табл.2*). Ця відмінність полягає у зростанні вірогідності перепаду яскравості елементів (*тобто тенденції збільшення структуризації текстури*) при збільшенні розмірності використовуваних блоків (в даному прикладі з 3 до 7 ел.). Причому в умовах обчислення локальної статистики *(P(1))*, ця тенденція є більш вираженою. В якості коментаря, такої нетипової поведінки спостережуваного процесу, можна припустити, що: - у разі обробки мнемосхем при збільшенні розмірів субблоків, зростає ймовірність «захвату» окремих ділянок контурів та/чи фрагментів об'єктів із однотонною заливкою (яскравістю)). Природно, що на малих блоках такий процес є менш виражений. І в першу чергу, така ситуація обумовлена саме природою таких зображень, що містять велику кількість однотонних областей і протяжних контурів виключно правильної форми, котрі формують основні об'єкти сцени, які відображаються. Очевидно, що при таких відмінних рисах цього типу зображень (рис.1(а)), варіювання порогом загрублення *«P_Z»* не призводить до таких специфічних наслідків. Вони

(наслідки) виявляться тільки при досягненні значень обраного порога *(P_Z)*, порівнянних з рівнем контрасту, що притаманний для основних контурів. А така ситуація є неприйнятною, з погляду завдань стеганографії, так як вихідне зображення зазнає неприпустимих змін свого вихідного стану. В цілому, отримані результати (табл.2) демонструють, що перехід від глобального до блокового розрахунку ймовірності покращує точність її оцінки для окремих ділянок зображень, з помітною тенденцією зменшення ймовірностей при збільшенні використовуваних блоків. Одержані відомості слугують основою для подальшого аналізу впливу параметрів обробки на якість перетворень зображень на наступних етапах алгоритму.

Слід зазначити, що процедури згладжування суттєво змінюють фактуру зображень, впливаючи на розподіл яскравості та градієнтів ймовірності її перепаду [10]. Зокрема, при щадному/слабкому згладжуванні (P_Z = 3-5), зберігається значна частка локальних перепадів, що відображається у декілька більших значеннях ймовірностей. Але з ростом верхньої межі припустимого загрублення яскравості (P_Z = 7-14) починається певне розмиття контурів й незначне зменшення деталізації, що призводить до виникнення на зображені візуально малопомітних артефактів у вигляді масштабування однорідних (схожих за структурою блоків) ділянок/фрагментів що, власне, і визначає процес зменшення ймовірність перепаду яскравості, порівняно з вихідним масивом зображення (див. рис. 3 в роботі [10]). Таким чином, «сильне» згладжування може призводити до втрати критичної інформації про структуру зображення, знижуючи його чіткість і, потенційно, погіршуючи результати подальшої сегментації чи розпізнавання об'єктів. Це підкреслює необхідність підтримки балансу між max можливими параметрами згладжування (значення *«N»* і *«P_Z»*) та збереженням потрібної деталізації оброблюваних зображень. Забезпечення цього балансу є ключовим аспектом для підтримки візуально незмінної якості оброблюваних зображень, особливо в задачах, що потребують точного розпізнавання об’єктів чи складних текстур цих зображень.

На рис. 2-4 представлені тестові зображення після застосування процедур 2-го варіанту згладжування, а також відповідні залежності кількості сформованих серій ОБ [17] на першому етапі алгоритму [4], в умовах застосування різних значень параметра P_Z. Ці візуалізації дозволяють наочно оцінити, яким чином параметри згладжування впливають на структуру й візуальну якість зображення та, в наступному, кількість серій ОБ (*вже з «власним» пороговим значенням, використовуваним при порівнянні вмісту сусідніх блоків*).

Представлені залежності (див. рис. 2-4(*ж,з*)) характеризують вплив розміру субблоків (*N*×*N*) і значення параметра «P_Z» на кількість сформованих серій ОБ для випадку розгортки типу *«По рядкам»* [4,11]. У цьому контексті аналіз наведених значень *PSNR* (пікове співвідношення сигнал/шум) дозволяє кількісно оцінити якість зображень після їх згладжування, що є важливим для кількісного порівняння різних підходів до обробки. Отримані результати свідчать про те, що коректний вибір параметрів передобробки (*контейнеру і контенту*) значно підвищує ефективність загального алгоритму, знижуючи його обчислювальну складність без помітних втрат у візуальної якості перетворених зображень. Безумовно, що використання малих розмірностей матриць згладжування вносить менший рівень спотворень (зразки (*а,в,д*) на рис.2-4) при збереженні хороших стартових умов для відпрацювання етапу формування серій ОБ (*гістограми (ж) на рис.2-4*). При цьому, залежно від типу зображення, різниця в кількості серій, що формуються (*див. гістограми (ж) і (з) на рис.2-4*) при різних розмірностях блоків, відрізняється найбільш істотним чином (в 4-6,5 рази). Однак, навіть така істотна відмінність у кількості формованих серій не зменшує цінність отриманого кінцевого ефекту: - створення умов для зниження обчислювальної складності алгоритму (на етапі кодування з перетворенням [4]) зі збереженням високої якості вихідного зображення. Як приклад, на мініатюрах (д) на Рис.2-4 представлені зразки з найкращим співвідношенням С/Ш (зелений фон). Відповідно, на зразках (*Рис.2-4(б), червоний фон*) відображені результати

обробки з найгіршою якістю відновлення для обраного діапазону налаштувань: - *N = 7, тобто великі блоки та P_Z = 3, тобто більша чутливість при порівнянні вибраних пар і, відповідно, велика кількість змін, що вносяться в вихідні значення яскравості*. Попарне порівняння зразків (д) і (б) знімає всі питання щодо якості одержуваного результату.

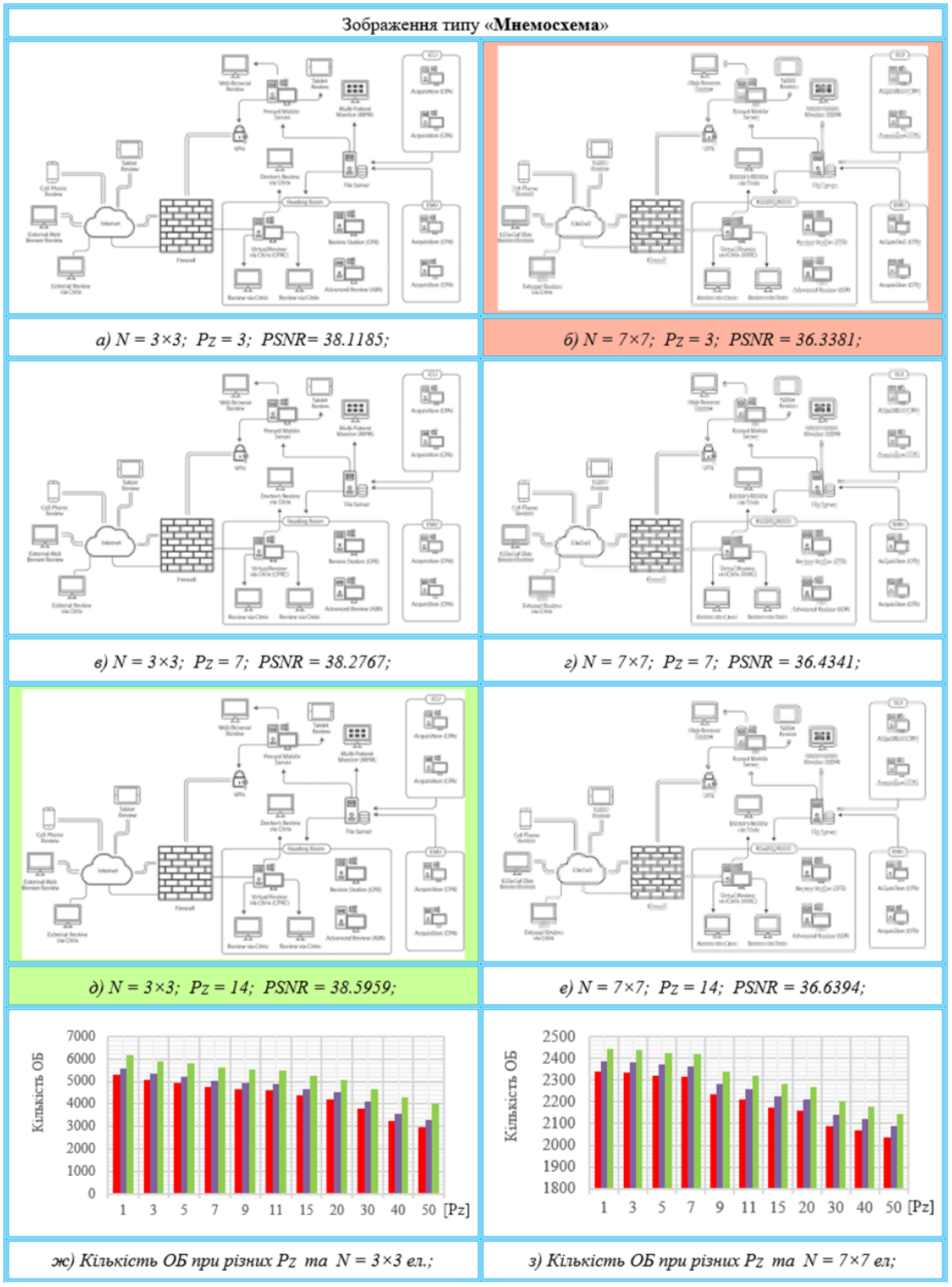


Рис. 2 – Кількість ОБ в зображенні *«**Мнемосхема**»* для різних блоків (N) і значень «P_Z»

*Fig. 2 – Number of BBs in the «**Mnemonic scheme**» image for different blocks (N) and «P_Z» values*

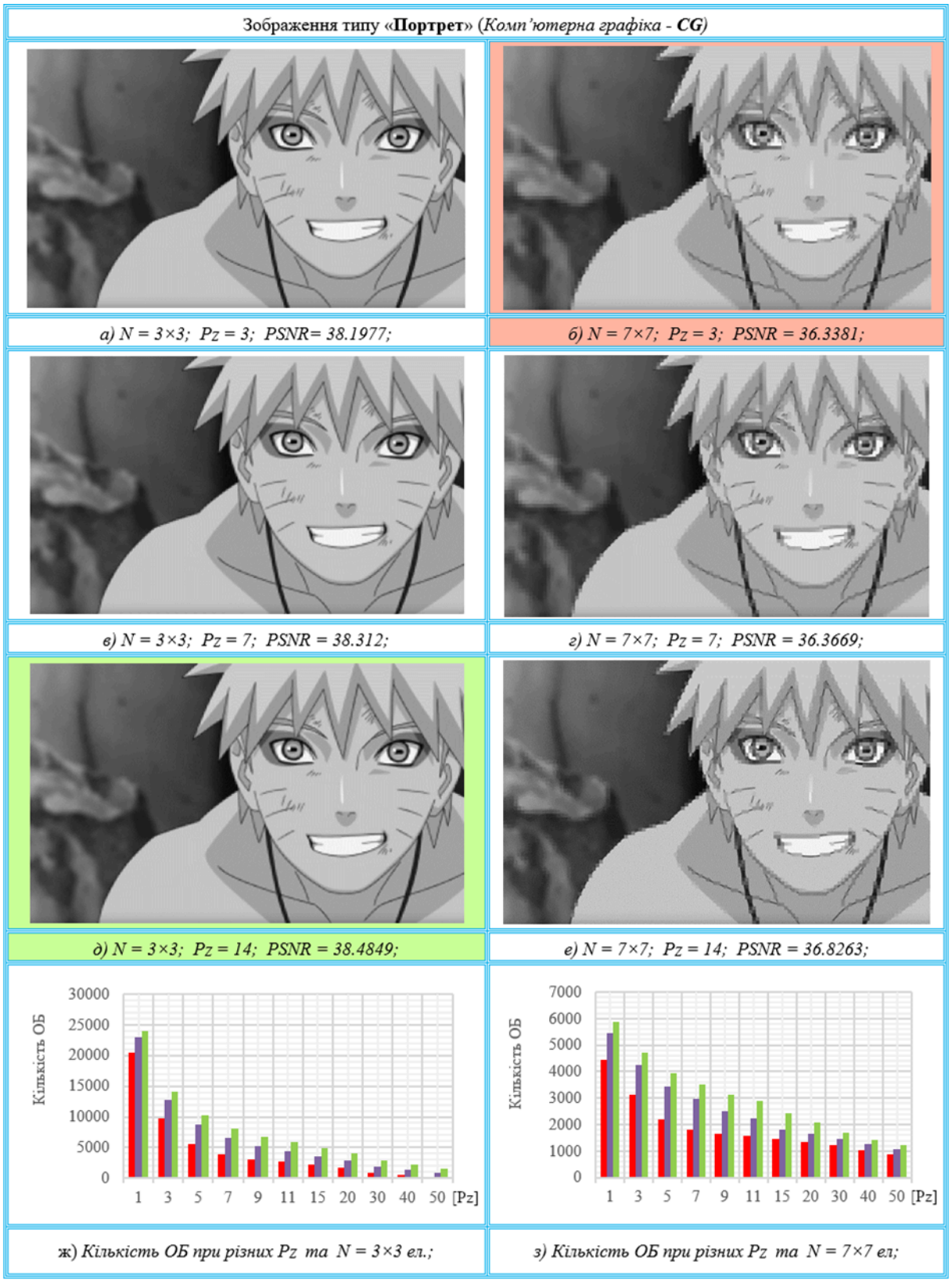


Рис. 3 – Кількість ОБ в зображенні *«**Портрет**»* для різних блоків (N) і значень «P_Z»

*Fig. 3 – Number of BBs in the «**Portrait**» image for different blocks (N) and «P_Z» values*

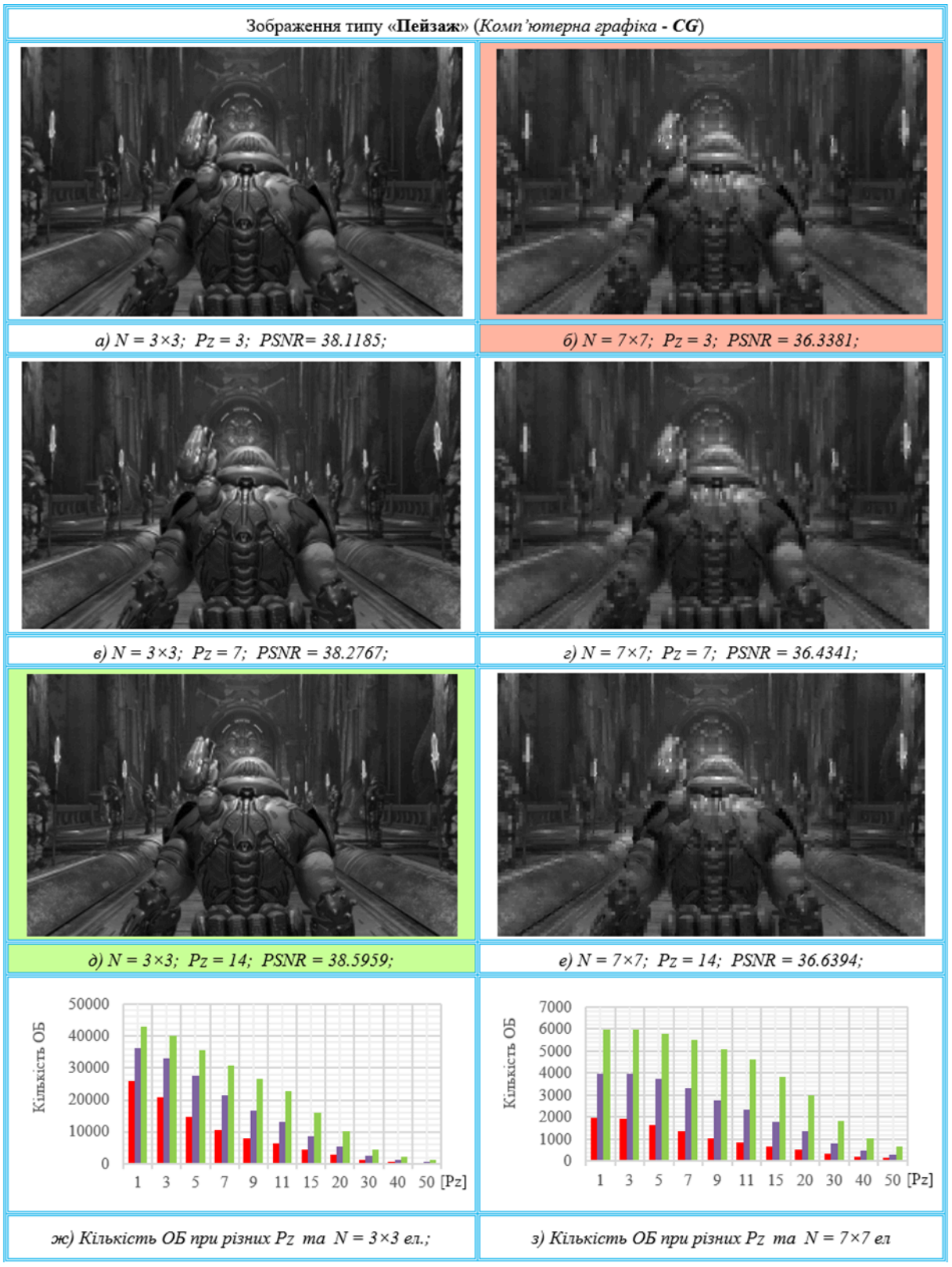
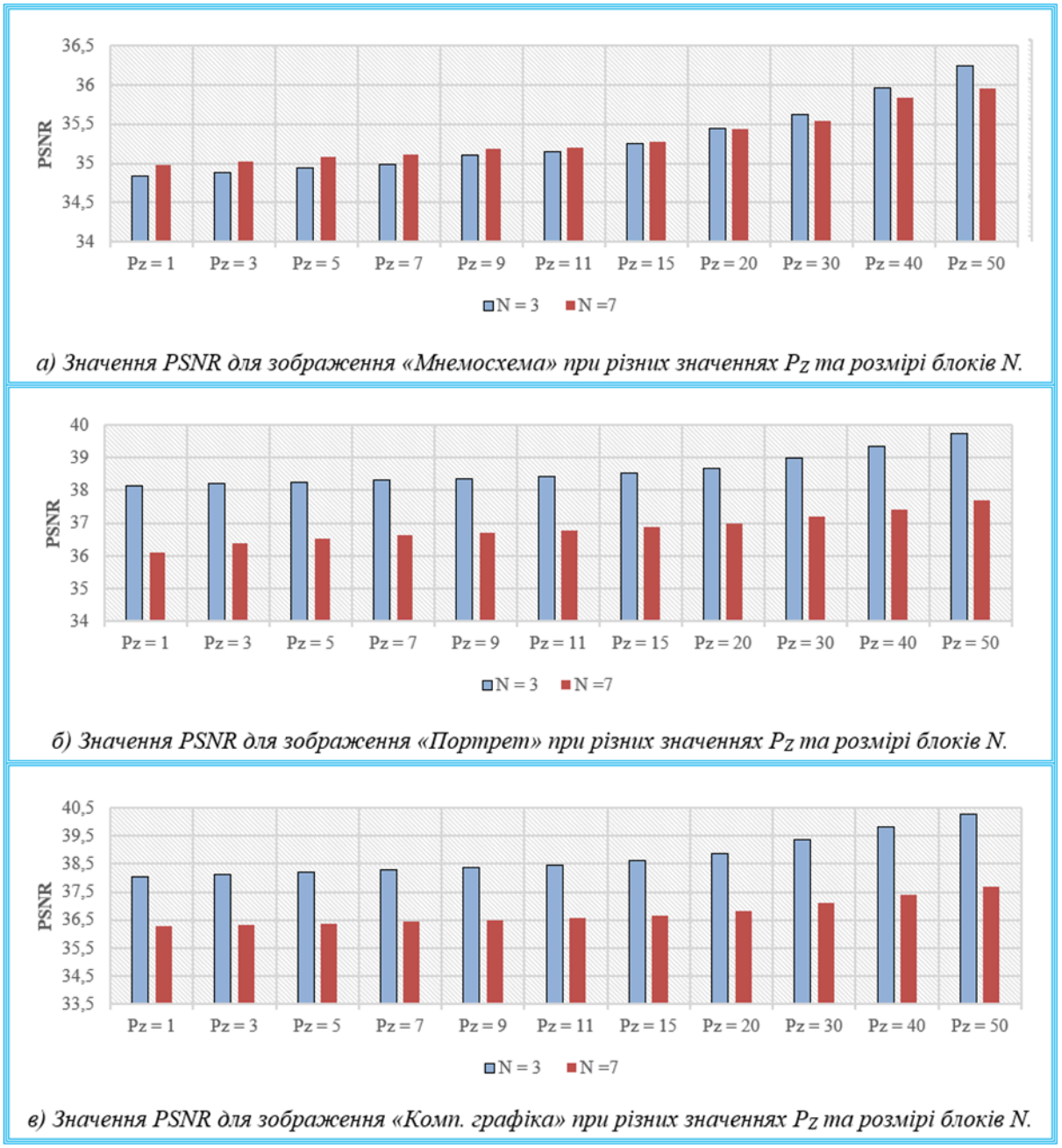


Рис. 4 – Кількість ОБ в зображенні *«**Пейзаж**»* для різних блоків (N) і значень «P_Z»
*Fig. 4 – Number of BBs in the «**Landscape**» image for different blocks (N) and «P_Z» values*

При цьому динаміка прогресу, в частині зменшення візуальних артефактів, добре простежується і в рамках кожного з окремо взятих стовпців на Рис.2-4.

На рис. 5 представлені гістограми значень *PSNR* [1,5,8] в залежності від різних параметрів обробки для 2-го варіанту згладжування. Ці результати додатково підтверджують необхідність збалансованого підходу до вибору діючих параметрів обробки, що забезпечує потрібний рівень згладжування текстури без втрати важливих деталей зображень.



а) Значення PSNR для зображення «Мнемосхема» при різних значеннях P_Z та розмірі блоків N.

б) Значення PSNR для зображення «Портрет» при різних значеннях P_Z та розмірі блоків N.

в) Значення PSNR для зображення «Комп. графіка» при різних значеннях P_Z та розмірі блоків N.

Рис. 5 – Значення PSNR в умовах зміни параметрів P_Z та N для 2-го варіанту згладжування

Fig. 5 – PSNR values in conditions of changing P_Z and N parameters for the 2nd smoothing variant

Отримані дані дозволяють оцінити ефективність різних способів обробки, визначити оптимальні параметри та досягти балансу між якістю зображення та обчислювальною складністю алгоритму для подальшої інкапсуляції даних. Це, у свою чергу, впливає на базу можливих перестановок для діючих параметрів серії та може підвищувати помітність

артефактів. При цьому ОБ більшої розмірності менш схильні до зростання кількості сформованих серій, ніж блоки малої розмірності [4].

Виходячи з наведених результатів, можна констатувати, що: - зменшення розмірності матриць згладжування (субблоків) та збільшення значення параметра P_Z, в умовах використання 2-го варіанту передобробки, призводять до зростання ймовірності перепаду яскравості (*див. табл.2*), тобто сприяють збереженню більш високої якості оброблюваних зображень, ніж за інших варіантів налаштувань.

Враховуючи природно складнішу структуру зображень типу ***«Пейзаж»*** (в даному разі Комп.Графіка (CG)), результат їх обробки дає безумовно більшу кількість формованих опорних блоків (тобто більше серій), порівняно з будь-якими іншими типами зображень (*див. фрейм (ж) на рис.2-4*). При цьому, зі збільшенням розмірності використовуваних субблоків, отриманий результат, за кількістю серій, зменшується в рази (*див. фрейми (ж) і (з) на рис.2-4*). Однак для більш цікавих, з точки зору застосовності стегановставки, зображень (***«Портрет»*** та ***«Пейзаж»***), використання на етапі передобробки, блоків малої розмірності дає однакову динаміку змін при практично збігающихся результатах обробки *(див. Рис.5 (б-в))*. Іншими словами, збільшення розмірності вікна згладжування, помітно погіршує якість вихідних зображень (*див. червоний фрейм (б) на рис.3-4*), проте дає суттєвий виграш зі зменшення часу обробки даних на наступних етапах алгоритму за рахунок значного зменшення кількості блоків, що вимагають їх обробки (дискретне косинусне перетворення [4,7]). Порівняння фреймів (ж) і (з) на рис. 2-4, наочно підтверджує цей факт.

В цілому, оптимальними параметрами налаштувань для забезпечення збалансованого ефекту між якістю отримуваних зображень, кількістю сформованих серій ОБ [12,17] та забезпечуваною обчислювальною ефективністю є: - розмірність матриць згладжування (субблоків) від 3 до 5 елементів та значення порогу загрублення P_Z у межах від 3 до 15 градацій яскравості. Саме такий діапазон налаштувань створює потрібні умови для формування масиву серій ОБ, що забезпечує потрібні перетворення на наступних етапах алгоритму [17]. Крім того, розширений аналіз всієї сукупності результатів моделювань показує, що обрані параметри згладжування сприяють високій адаптивності алгоритму до різного ступеня деталізації зображень [4]. Це дозволяє ефективно масштабувати розглянуті механізми для обробки не лише класичних типів зображень [7], а й для інших, варіацій візуального контенту (наприклад, штучно створених зображень типу *«Комп'ютерна Графіка»* (рис.3-4), з притаманними до них особливостями текстури). Така процедурна адаптивність відкриває широкі можливості для подальших досліджень і вдосконалення розроблених підходів до обробки зображень з урахуванням їхнього змісту та одержуваного статистичного диспаритету в динамічній системі комбінаторних пар *«контент – контейнер»*, що створює необхідні передумови для розробки більш гнучких і енергоефективних алгоритмів стегановставки, пристосованих для роботи в різних умовах (обмеженнях) та з широкою номенклатурою вихідних даних.

4. Висновки

1. Використання різних варіантів попередньої обробки вихідних даних на початкових етапах алгоритму стегановставки, забезпечує необхідні передумови для формування однорідних серій ОБ, що є фактором впливу для подальшої ефективної інкапсуляції даних та покращення стійкості контенту до спроб його неавторизованого вилучення [3, 11-17].

2. Результати згладжування вихідних текстур та кількість формованих серій ОБ, залежать від типу зображень, розмірності блоків, порогу загрублення (P_Z), використаної схеми розгортки [11,13,15] та обраного варіанту згладжування [4], що дозволяє адаптувати алгоритм до різних сценаріїв дій та ресурсних обмежень.

3. Використання різних схем розгортки серій ОБ відіграє ключову роль у забезпеченні компромісу між складністю реалізації алгоритму, його захисним потенціалом та обчислювальною ефективністю [11-16]. Схема розгортки визначає спосіб вибірки потрібних параметрів зображень, впливаючи на формування масиву ОБ та структуру викривлень атакованих зображень, що ускладнює неавторизовану екстракцію контенту. Таким чином, вибір схеми розгортки є критичним для балансу між безпекою та ефективністю алгоритму.

4. Ймовірність перепаду яскравості є ключовим параметром у цифровій обробці зображень [7]. Цей параметр дає змогу аналізувати текстурні та колірні характеристики зображень, виявляти зміни яскравості/кольору між сусідніми пікселями, а також оцінювати текстурну неоднорідність окремих ділянок зображень. Його використання сприяє вдосконаленню методів передобробки зображень, забезпечуючи кращу адаптацію алгоритмів до специфічних умов обробки, зокрема для задач стеганографії. Крім того, аналіз ймовірності перепаду яскравості дозволяє оптимізувати процеси сегментації зображень і виявлення об’єктів, що підвищує загальну ефективність і точність алгоритмів обробки зображень.

5. Збільшення верхньої межі загрублення параметру *«P_Z»* на етапі передобробки вихідних даних, для будь-якої розмірності блоків, неминуче призводить до погіршення ефекту вирівнювання їх вихідної текстури. Тобто, ефект згладжування значно більшою мірою залежить від використовуваної розмірності блоків та обраного варіанту їх обробки, ніж від тенденції збільшення параметра *«P_Z»*.

6. Оцінка обчислювальної складності процедур згладжування показує, що 1-й та 2-й варіанти мають однакову асимптотичну складність. Вони демонструють квадратичну обчислювальну складність $O(M^2)$, що робить їх оптимальними для систем з обмеженими ресурсами, забезпечуючи достатній рівень однорідності при помірних обчислювальних витратах. Третій варіант, зі складністю $O(M^2 \times N^2)$, забезпечує найвищу якість згладжування, але є непрактичним для великих зображень чи блоків, через високу ресурсомісткість, що обмежує його використання в реальних сценаріях дій.

7. Вибір параметрів попередньої обробки вихідних зображень (контейнеру й контенту) відіграє ключову роль у досягненні потрібного балансу отримуваних результатів. Оскільки зображення характеризуються різними текстурами та значними варіаціями деталей, тому правильне налаштування параметрів дозволяє чітко розділяти важливі елементи між основними деталями та фоновими ділянками. Це значно покращує якість інкапсуляції контенту, зменшуючи помітність артефактів і підвищуючи стійкість до виявлення прихованих даних.

8. Оптимальні значення розмірності блоків N від 3 до 5 та порогу загрублення P_Z від 3 до 15 забезпечують баланс між збереженням візуальної якості зображень з різним контентом та ефективністю формування серій ОБ. Крім того, адаптивне згладжування малоінформативних областей, сприяє створенню однорідних блоків, що ускладнює статистичний аналіз і підвищує місткість контейнера для приховування інформації.

9. Варіювання розміром маски згладжування та типом зображення-контейнера дозволяє досягти компромісу між допустимим рівнем спотворень і кількістю сформованих ОБ [3]. Це забезпечує гнучкість у налаштуванні варіантів мультиплексування даних, де кожен рівень відповідає певній позиції в структурі композитного ключа екстрактора даних [3,17].

10. У подальшому планується провести експериментальну оцінку складності виконуваних процедур для різних схем розгортки й просторової орієнтації ОБ [11,13], що дозволить визначити загальні умови і обмеження, які впливають на забезпечення ресурсного консенсусу при обробці різних типів даних у комбінаторній системі *«контент–контейнер»*.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

Список літератури

1. Fridrich, J. (2010). *Steganography in digital media*. Cambridge University Press.
2. Hassaballah, M. (Ed.). (2020). *Digital media steganography: Principles, algorithms, and advances*. Academic Press.
3. Honcharov, M., & Malakhov, S. (2024). Modeling attempts of unauthorized extraction of steganocontent under different combinations of data key-extractor. *Débats scientifiques et orientations prospectives du développement scientifique* (pp. 234–245). https://doi.org/10.36074/logos-01.03.2024.053
4. Гончаров, М. О., & Малахов, С. В. (2021). Моделювання процедур підготовки даних стеганоалгоритма з багаторівневим мультиплексуванням контенту. *Комп'ютерне моделювання в наукоємних технологіях (КНМТ-2021): Матеріали 7-ї міжнар. наук.-техн. конф.* (pp. 118–122). ХНУ ім. В. Н. Каразіна. http://surl.li/axsna
5. Конахович, Г., Прогонов, Д., & Пузиренко, О. (2018). *Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних*: Підручник. Центр навчальної літератури.
6. Shih, F. Y. (2020). *Digital watermarking and steganography*. CRC Press.
7. Pratt, W. K. (1978). *Digital image processing*. New York: John Wiley & Sons.
8. Кузнецов, О. О., Євсеєв, С. П., & Король, О. Г. (2011). *Стеганографія*: навч. посіб. Харків: Видавництво ХНЕУ.
9. Yahya, A. (2019). *Steganography techniques for digital images*. Springer International Publishing.
10. Малахов, С., & Гончаров, М. (2024). Синтез ймовірнісних карт переходів яскравості (градієнтів) зображень для покращення процедур стегановставки. Grail of Science, (47), 545–554. https://archive.journal-grail.science/index.php/2710-3056/issue/view/20.12.2024/35
11. Гончаров, М., & Малахов, С. (2023). Дослідження способів розгортки вихідних блоків зображення - стеганоконтенту як механізму протидії від несанкціонованої екстракції даних. *Science and Technology Today*, 4(18), 293–308. https://doi.org/10.52058/2786-6025-2023-4(18)-293-308
12. Малахов, С., Нарєжній, О., & Гончаров, М. (2023). Властивості серій опорних блоків стеганоконтенту та наслідки його несанкціонованого вилучення для різних схем розгортки серій. *Grail of Science*, (18-19), 204–211. https://archive.journal-grail.science/index.php/2710-3056/issue/view/07.07.2023/17
13. Гончаров, М., Малахов, С., & Колованова, Є. (2024). Результати моделювання різних схем просторової орієнтації та розгортки серій опорних блоків зображень для протидії несанкціонованої екстракції стеганографічних даних. *Комп'ютерні науки та кібербезпека*, (2), 58–70. https://doi.org/10.26565/2519-2310-2023-2-06
14. Лєсная, Ю., Гончаров, М., Азаров, С., & Малахов, С. (2023). Візуалізація спроб несанкціонованої екстракції стеганоконтенту при помилковому визначенні діючих способів розгортки серій. *Grail of Science*, (24), 335–340. https://doi.org/10.36074/grail-of-science.17.02.2023.061
15. Лєсная, Ю., Гончаров, М., Семенов, А., & Малахов, С. (2023). Моделювання розгортки серій опорних блоків зображення, як інструменту з протидії спробам несанкціонованої екстракції стеганоконтенту. *Collection of Scientific Papers «ΛΌГОΣ»*, (March 31, 2023; Zurich, Switzerland), 109–115. https://doi.org/10.36074/logos-31.03.2023.33
16. Малахов, С., & Гончаров, М. (2024). Уточнення процедур формування серій опорних блоків зображень на етапі їх передобробки при реалізації процедур стегановставки. Grail of Science, (46), 694–700. https://archive.journal-grail.science/index.php/2710-3056/issue/view/29.11.2024/34
17. Лєсная, Ю., Гончаров, М., & Малахов, С. (2021). Відпрацювання концепту багаторівневого мультиплексу даних гібридного стеганоалгоритму. Збірник наукових праць SCIENTIA. https://ojs.ukrlogos.in.ua/index.php/scientia/article/view/17666

MODELING AND EVALUATION OF THE COMPUTATIONAL COMPLEXITY OF THE MAIN PROCEDURES, THE INITIAL STAGES OF THE HYBRID STEGANOGRAPHIC ALGORITHM

Mykyta Honcharov[1], postgraduate student of the Department of Cybersecurity of Information Systems, Networks and Technologies; e-mail: m.honcharov@student.karazin.ua; ORCID: https://orcid.org/0000-0002-9790-7260
Serhii Malakhov[1], Ph.D., Senior Researcher, Associate Professor of the Department of Cybersecurity of Information Systems, Networks and Technologies; e-mail: malakhov@karazin.ua; ORCID: https://orcid.org/0000-0001-8826-1616
[1]*V. N. Karazin Kharkiv National University, Ukraine*
Manuscript was received March 1, 2025; Received after review April 1, 2025;
Accepted May 2, 2025

Abstract. In today's environment of increasing cyber threats, steganography plays a key role in ensuring data confidentiality by hiding it in digital data arrays (images, sound, file systems, etc.). Unlike cryptography, steganography hides the very fact of information transfer, which makes it indispensable for data protection in information and communication systems with limited resources. The need to create energy-efficient and adaptive algorithms that combine content robustness, high container quality, and low computational complexity emphasizes the relevance of the research conducted. The paper evaluates the computational complexity of input data preprocessing procedures and determines their impact on the efficiency of subsequent data encapsulation. As a basis for modeling, one of the possible variants of smoothing low-informative areas of the source images was selected. The following assessments were carried out: - performance by execution time for different types of images; PSNR metric; probability of color brightness difference and number of formed basic blocks (BBs) of images. During the modeling, the consequences of smoothing the textures of the source images were investigated in the conditions of varying smoothing matrix sizes and the value of the pixel brightness difference. The number of basic operations (arithmetic, logical, comparisons) for each block was calculated and the overall complexity of the corresponding stages of the algorithm was determined. The experimental evaluation was performed by measuring the execution time of the procedures, evaluating the image quality using the PSNR metric, calculating the probability of brightness difference, and counting the number of formed series of BBs. To evaluate the effectiveness of the investigated procedures, test images with different textural characteristics were used. The obtained results confirmed that the pre-smoothing stage improves the initial conditions for the formation of BBs series (compared to their absence). The introduction of the smoothing stage ensures noise reduction in low-information areas, which contributes to increased block homogeneity and expands the range of combinatorics of available encoding parameters (as a way to counteract attempts at unauthorized content extraction). Flexible settings for block size and brightness coarsening threshold values for image elements allow the smoothing process to be adapted to different image types and the current resource limitations of the hardware platforms used. The proposed approach to preprocessing data creates the necessary conditions for forming BBs series, improves content robustness, and maintains a low level of visual distortion. Adaptive settings for smoothing parameters allow the algorithm to be used effectively on platforms with limited resources.

Keywords: *information security, threats, cyberattack, computational complexity, data encapsulation, unauthorized access, steganography, run-length encoding*

Conflicts of Interest: the authors declare no conflict of interest.

References

1. Fridrich, J. (2010). *Steganography in digital media*. Cambridge University Press.
2. Hassaballah, M. (Ed.). (2020). *Digital media steganography: Principles, algorithms, and advances*. Academic Press.
3. Honcharov, M., & Malakhov, S. (2024). Modeling attempts of unauthorized extraction of steganocontent under different combinations of data key-extractor. *Débats scientifiques et orientations prospectives du développement scientifique* (pp. 234–245). https://doi.org/10.36074/logos-01.03.2024.053
4. Honcharov, M. O., & Malakhov, S. V. (2021). *Modeling data preparation procedures for a steganographic algorithm with multilevel content multiplexing*. Computer Modeling in High-Tech Technologies (KMNT-2021): Proceedings of the 7th International Scientific and Technical Conference (pp. 118–122). V. N. Karazin Kharkiv National University [in Ukrainian] http://surl.li/axsna
5. Konakhovych, H., Prohonov, D., & Puzyrenko, O. (2018). *Computer steganographic processing and analysis of multimedia data: Textbook*. Center for Educational Literature [in Ukrainian]
6. Shih, F. Y. (2020). *Digital watermarking and steganography*. CRC Press.
7. Pratt, W. K. (1978). *Digital image processing*. New York: John Wiley & Sons.
8. Kuznetsov, O. O., Yevseyev, S. P., & Korol, O. H. (2011). *Steganography: A textbook*. Kharkiv: KhNEU Publishing House [in Ukrainian]
9. Yahya, A. (2019). *Steganography techniques for digital images*. Springer International Publishing.
10. Malakhov, S., & Honcharov, M. (2024). *Synthesis of probabilistic brightness (gradient) transition maps of images to improve steganographic embedding procedures*. *Grail of Science*, (47), 545–554 [in Ukrainian] https://archive.journal-grail.science/index.php/2710-3056/issue/view/20.12.2024/35
11. Honcharov, M., & Malakhov, S. (2023). *Investigation of methods for unfolding original image blocks—steganocontent as a mechanism for counteracting unauthorized data extraction*. *Science and Technology Today*, 4(18), 293–308 [in Ukrainian] https://doi.org/10.52058/2786-6025-2023-4(18)-293-308
12. Malakhov, S., Narezhnyi, O., & Honcharov, M. (2023). *Properties of reference block series in steganocontent and consequences of its unauthorized extraction for different series unfolding schemes*. *Grail of Science*, (18-19), 204–211 [in Ukrainian] https://archive.journal-grail.science/index.php/2710-3056/issue/view/07.07.2023/17
13. Honcharov, M., Malakhov, S., & Kolovanova, Ye. (2024). *Modeling results of various spatial orientation schemes and unfolding of reference image block series to counter unauthorized extraction of steganographic data*. *Computer Science and Cybersecurity* (2), 58–70 [in Ukrainian] https://doi.org/10.26565/2519-2310-2023-2-06
14. Lesnaia, Yu., Honcharov, M., Azarov, S., & Malakhov, S. (2023). *Visualization of attempts at unauthorized extraction of steganocontent due to incorrect identification of active series unfolding methods*. *Grail of Science*, (24), 335–340 [in Ukrainian] https://doi.org/10.36074/grail-of-science.17.02.2023.061
15. *Lesnaia, Yu., Honcharov, M., Semenov, A., & Malakhov, S. (2023). Modeling the unfolding of reference image block series as a tool to counter attempts at unauthorized extraction of steganocontent. Collection of Scientific Papers «ΛΟΓΟΣ»*, (March 31, 2023; Zurich, Switzerland), 109–115 [in Ukrainian] https://doi.org/10.36074/logos-31.03.2023.33
16. Malakhov, S., & Honcharov, M. (2024). *Refinement of procedures for forming series of reference image blocks at the preprocessing stage during the implementation of steganographic embedding procedures*. Grail of Science, (46), 694–700 [in Ukrainian] https://archive.journal-grail.science/index.php/2710-3056/issue/view/29.11.2024/34
17. Lesnaia, Yu., Honcharov, M., & Malakhov, S. (2021). *Development of the concept of multilevel data multiplexing in a hybrid steganographic algorithm*. *Collection of Scientific Papers* SCIENTIA [in Ukrainian] https://ojs.ukrlogos.in.ua/index.php/scientia/article/view/17666

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 1 (27)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 1 (27)

DOI: https://doi.org/10.26565/2519-2310-2025-1-05
УДК 340.137

ДОСЛІДЖЕННЯ ТА ПОРІВНЯННЯ НОРМАТИВНИХ РЕГУЛЯТОРНИХ ДОКУМЕНТІВ ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ КІБЕРБЕЗПЕКИ

Марина Єсіна[1,2], канд. техн. наук, доцент, в.о. завідувача кафедри кібербезпеки інформаційних систем, мереж і технологій, ННІ КШ та ШІ; науковий співробітник-консультант, e-mail: m.v.yesina@karazin.ua, ORCID: https://orcid.org/0000-0002-1137-2382

Єлизавета Логачова[1], студентка 5 курсу кафедри кібербезпеки інформаційних систем, мереж і технологій, ННІ КШ та ШІ, e-mail: lohachova2020kb11@student.karazin.ua, ORCID: https://orcid.org/0000-0002-9815-466X

Євгенія Колованова[1], канд. техн. наук, в.о. заступника директора з навчальної роботи, ННІ КШ та ШІ, e-mail: e.kolovanova@karazin.ua, ORCID: https://orcid.org/0000-0002-0326-2394

[1]Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна

[2]ПрАТ "Інститут Інформаційних Технологій", вул. Отамановського професора, 15, Харків, 61022, Україна

Рукопис надійшов 1 березня 2025 р. Отримано після рецензування 1 квітня 2025 р. Прийнято 2 травня 2025 р.

Анотація: У статті представлено ґрунтовне дослідження та порівняння основних нормативно-правових актів Європейського Союзу у сфері кібербезпеки, серед яких: Директива NIS2, Загальний регламент про захист даних (GDPR), Регламент про цифрову операційну стійкість (DORA) та стандарт PCI DSS. Ці документи розглядаються як основоположні елементи формування сучасної політики ЄС у сфері захисту цифрової інформації, що охоплює персональні дані, фінансову інформацію та критичну інфраструктуру. У роботі окреслено ключові завдання кожного з актів, проаналізовано їхню сферу застосування, вимоги до суб'єктів регулювання, механізми управління ризиками, звітування про інциденти, взаємодію з постачальниками, а також санкційні положення. Особливу увагу приділено порівнянню актів за впливом на бізнес та IT-інфраструктуру, а також виявленню взаємозв'язків між ними. Встановлено, що хоча кожен документ має власний фокус - захист персональних даних, стійкість фінансової інфраструктури, безпека цифрових мереж чи захист транзакцій з платіжними картками – всі вони спрямовані на створення цілісної екосистеми кіберзахисту в межах ЄС. Стаття також аналізує міжнародні аналоги згаданих актів, такі як GDPR-подібні закони у США та Бразилії, стандарти NIST та ISO, що свідчить про глобальний характер проблеми цифрової безпеки та пошук спільних підходів до її вирішення. У підсумку, робота підкреслює важливість комплексного та гармонізованого підходу до кібербезпеки як ключової умови сталого розвитку цифрового суспільства. З огляду на актуальні загрози, зокрема геополітичні конфлікти та зростання масштабів кіберзлочинності, ефективна імплементація європейських стандартів набуває особливого значення для країн-партнерів, зокрема України, яка потребує адаптації відповідних норм для підвищення національної кіберстійкості.

Ключові слова: *нормативні документи, європейський союз, регуляторні документи, кібербезпека, бізнес, захист інформації*

Як цитувати: Єсіна М., Логачова Є., Колованова Є. Дослідження та порівняння нормативних регуляторних документів європейського союзу у сфері кібербезпеки. *Комп'ютерні науки та кібербезпека.* 2025; № 1(27): С. 60–72. https://doi.org/10.26565/2519-2310- 2025-1-05

In cites: Yesina M., Lohachova Ye., Kolovanova Ye. (2025). Research and comparison of European Union regulatory documents in cybersecurity. *Computer Science and Cybersecurity. 1*(27): 60–72. https://doi.org/10.26565/2519-2310- 2025-1-05 (in Ukrainian)

1. Вступ

У сучасному світі цифрові технології стали невід'ємною складовою суспільного, економічного та політичного життя. Разом із безпрецедентними можливостями, які вони відкривають для розвитку економік та суспільств, вони також створюють нові загрози – від кібершахрайства до масових атак на критичну інфраструктуру. У цьому контексті питання кібербезпеки набуло особливої ваги як на національному, так і на міжнародному рівнях. Європейський Союз, як одне із провідних інтеграційних об'єднань у світі, визначає кібербезпеку як пріоритетний напрямок своєї політики, прагнучи створити високий рівень кіберзахисту для своїх громадян, бізнесу та державних інституцій.

Нормативно-правове регулювання кібербезпеки в ЄС є багаторівневим та динамічним процесом. Його розвиток відображає прагнення країн-членів забезпечити як надійний захист критичної інфраструктури та персональних даних, так і сталий розвиток цифрової економіки. З цією метою ЄС прийняв низку важливих нормативно-правових актів, серед яких особливе місце займають Директива NIS та її оновлена версія – NIS2, GDPR, DORA, а також PCI DSS [1-4]. Кожен із цих документів має свою сферу застосування, особливості та завдання, однак усі вони спрямовані на досягнення спільної мети – забезпечення кіберстійкості та цифрової довіри в Європейському Союзі.

Аналіз та порівняння цих нормативних актів дозволяє глибше зрозуміти, якими шляхами ЄС намагається врегулювати питання кібербезпеки, ураховуючи постійні технологічні зміни та еволюцію кіберзагроз. Особливої актуальності це набуває в умовах геополітичних викликів, зокрема в контексті агресії російської федерації проти України, що ще більше підкреслило важливість кібербезпеки для захисту державних інституцій та критичних сервісів.
Метою цієї статті є дослідження та порівняння основних нормативно-правових документів Європейського Союзу у сфері кібербезпеки, визначення їхніх спільних рис та відмінностей, а також аналіз впливу на держави-члени та бізнес.

2. Ключові нормативно-правові документи ЄС

Атаки на основі ШІ можна класифікувати за багатьма різними параметрами. Так, наприклад, кілька систем класифікації атак були представлені в роботах [7, 8]. Також NIST в своєму звіті щодо атак на машинне навчання ШІ представив різні типи класифікації [1, 25]. В цьому розділі будуть розглянуті деякі типи класифікацій.

2.1. Директива NIS2 та її особливості

CNIS2 Directive (Network and Information Security Directive 2) – це оновлена структура Європейського Союзу з кібербезпеки, яка замінює оригінальну Директиву NIS (2016) [1]. Вона розроблена для посилення кібербезпеки в Європейському Союзі шляхом встановлення високого загального рівня безпеки для мережевих та інформаційних систем. Її основною метою є

посилення кіберстійкості критичних секторів, а також забезпечення уніфікованих стандартів кіберзахисту для всіх суб’єктів цифрової економіки, незалежно від їхньої галузі та розміру.

Директива ставить за мету кілька ключових завдань, які разом утворюють системний підхід до кібербезпеки. Насамперед це зміцнення можливостей держав-членів у сфері кібербезпеки, що передбачає розвиток національних стратегій, створення компетентних органів та ефективних механізмів реагування на інциденти. Другим важливим завданням є покращення співпраці між державами-членами, що сприяє своєчасному обміну інформацією про кіберзагрози та координації дій у випадку масштабних атак. Ще одна мета – зменшення фрагментації на внутрішньому ринку ЄС, адже різні підходи до регулювання в окремих країнах створювали прогалини у захисті цифрової інфраструктури. Нарешті, Директива запроваджує обов’язкові вимоги з управління ризиками та звітування про кіберінциденти, що суттєво посилює відповідальність організацій за стан кібербезпеки [1].

Основні вимоги Директиви охоплюють кілька напрямків. Перш за все, це управління ризиками, яке передбачає впровадження суб’єктами (операторами основних послуг та постачальниками цифрових послуг) технічних, операційних та організаційних заходів. До таких заходів належать [1]: систематичний аналіз ризиків та розробка політики безпеки; ефективне реагування на інциденти; забезпечення безперервності бізнесу та планування відновлення після інцидентів; безпека закупівель та використання ІТ-систем; а також політика моніторингу, тестування та аудитів кібербезпеки.

Другим важливим компонентом є звітування про інциденти. Відповідно до Директиви, суттєві інциденти повинні бути повідомлені до відповідних компетентних органів протягом 24 годин з моменту їх виявлення. При цьому організація має надати повне повідомлення про інцидент не пізніше, ніж через 72 години, а остаточний звіт – не пізніше, ніж через один місяць після події. Такий підхід дозволяє державним органам оперативно реагувати на інциденти, координувати дії між суб’єктами ринку та зменшувати потенційний вплив на суспільство [1].

Окрему увагу Директива приділяє постачальникам ІКТ-послуг, встановлюючи обов’язок оцінки та контролю ланцюга постачання. Це означає, що організації повинні впроваджувати заходи безпеки для забезпечення надійності своїх партнерів та контрагентів, а також враховувати кіберризики у договірних відносинах із критичними постачальниками. Такий підхід допомагає створити більш стійку екосистему цифрових послуг у межах ЄС [1].

Важливою особливістю NIS2 є посилення ролі керівних органів. Відтепер вони несуть відповідальність за схвалення та нагляд за впровадженням заходів кібербезпеки у своїх організаціях. У разі недотримання вимог Директиви керівники можуть бути притягнуті до відповідальності, що підкреслює важливість кібербезпеки як стратегічного питання для кожної компанії [1].

Зрештою, кожна держава-член ЄС зобов’язана призначити національні компетентні органи, які здійснюють нагляд за виконанням вимог Директиви. Це сприяє уніфікації підходів до моніторингу та контролю в межах ЄС, а також створює механізми ефективної взаємодії між країнами у сфері кібербезпеки.

2.2. Регламент GDPR та його особливості

General Data Protection Regulation (GDPR) – це Загальний регламент про захист даних, прийнятий Європейським Союзом і такий, що набув чинності 25 травня 2018 року [2]. Він є ключовим нормативним документом, який визначає правила обробки персональних даних громадян ЄС. Особливість цього документа полягає в його екстериторіальній дії: правила GDPR поширюються не лише на організації, що перебувають у межах Європейського Союзу, але й на будь-які компанії, що обробляють персональні дані громадян ЄС, незалежно від місця їхньої

реєстрації [2]. У такий спосіб GDPR суттєво підвищує рівень захисту персональних даних і гарантує громадянам ЄС контроль над тим, як їхні дані збираються та використовуються.

Основними принципами, на яких базується GDPR, є законність, справедливість і прозорість обробки даних [2]. Це означає, що персональні дані повинні оброблятися на законних підставах, чесно та прозоро для суб'єкта даних. Наприклад, компанія має чітко повідомити людині, які дані збираються, для чого вони потрібні та як довго їх планують зберігати. Це створює довіру між користувачем і організацією та забезпечує право особи знати, що відбувається з її персональними даними.

Іншим ключовим принципом є обмеження мети: персональні дані повинні збиратися лише для конкретних, явних і законних цілей та не можуть оброблятися далі у спосіб, несумісний з цими цілями. Наприклад, якщо компанія збирає електронні адреси для реєстрації в сервісі, вона не має права використовувати ці дані для нав'язливої реклами без додаткової згоди користувача [2].

Мінімізація даних означає, що організації повинні збирати лише ті дані, які справді необхідні для досягнення задекларованих цілей. Таким чином, збір надлишкових даних забороняється, що запобігає зловживанням та підвищує безпеку особистої інформації. Принцип точності вимагає від організацій забезпечити актуальність даних: інформація повинна бути точною й оновлюватися за потреби [2]. Це важливо, щоб уникнути помилок або використання застарілих даних, що можуть призвести до порушення прав особи.

Принцип обмеження зберігання вказує на те, що персональні дані не повинні зберігатися довше, ніж це необхідно для досягнення цілей обробки [2]. Організації мають визначати строки зберігання даних і знищувати або анонімізувати їх після завершення обробки. Це суттєво знижує ризики витоку інформації та зловживання.

Цілісність і конфіденційність є одними з найважливіших вимог GDPR, оскільки вони вимагають забезпечити належну безпеку персональних даних, у тому числі їх захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення чи пошкодження. Організації повинні впроваджувати технічні та організаційні заходи безпеки, такі як шифрування, регулярне резервне копіювання та контроль доступу, щоб гарантувати безпеку даних [2].

GDPR застосовується до організацій, розташованих у межах ЄС, які обробляють персональні дані. Крім того, його вимоги поширюються й на організації, що перебувають за межами ЄС, якщо вони пропонують товари чи послуги громадянам ЄС або моніторять поведінку осіб у межах ЄС [2]. Таким чином, навіть компанії, що не мають фізичної присутності в ЄС, підпадають під дію GDPR, якщо вони працюють із громадянами ЄС.

Порушення вимог GDPR може призвести до накладення значних штрафів, які становлять до 20 мільйонів євро або до 4% річного світового обороту компанії – залежно від того, яка сума є більшою [2]. Такі фінансові санкції стимулюють компанії дотримуватися принципів прозорої, законної та безпечної обробки персональних даних, а також створюють новий рівень відповідальності для бізнесу в цифровому середовищі.

2.3. Регламент DORA та його особливості

Digital Operational Resilience Act (DORA) – це Регламент Європейського Союзу, спрямований на посилення цифрової стійкості фінансового сектору. Він набув чинності 16 січня 2023 року, а його застосування розпочалось 17 січня 2025 року [3]. Цей регламент є ключовим кроком ЄС у забезпеченні стійкості фінансових установ до ризиків, пов'язаних із інформаційними та комунікаційними технологіями (ІКТ), зокрема кіберінцидентами та технічними збоями. DORA створює єдиний стандарт цифрової операційної стійкості для всіх

фінансових організацій, щоб гарантувати їхню здатність витримувати, реагувати та відновлюватися після порушень у сфері ІКТ [3].

Однією з основних вимог DORA є управління ІКТ-ризиками, яке передбачає, що фінансові установи повинні впроваджувати комплексні рамки управління ризиками. Це включає ідентифікацію ризиків, їхню профілактику, своєчасне виявлення інцидентів, ефективне реагування та відновлення після подій [3]. Такий підхід дозволяє організаціям підготуватися до потенційних кіберзагроз та забезпечує безперервність надання фінансових послуг навіть під час кризових ситуацій.

Регламент також запроваджує обов’язкове звітування про інциденти: фінансові установи повинні повідомляти національні регуляторні органи про значні інциденти у сфері ІКТ. Це дозволяє державним органам оперативно реагувати на інциденти та координувати заходи для запобігання системним ризикам у фінансовому секторі [3]. Таким чином, DORA сприяє своєчасному обміну інформацією та знижує ризики поширення кіберзагроз.

Ще однією важливою вимогою є регулярне тестування цифрової операційної стійкості, яке передбачає проведення як базових, так і передових тестувань для певних установ [3]. Це допомагає визначити слабкі місця у системах та процесах організацій, а також забезпечити їхню готовність до реагування на кіберінциденти. Регулярні тренування та симуляції атак підвищують загальну кіберстійкість фінансової екосистеми ЄС.

Крім того, DORA передбачає управління ризиками третіх сторін. Фінансові установи зобов’язані встановлювати вимоги до ІКТ-постачальників, укладати відповідні контракти та забезпечувати належний моніторинг їхньої діяльності [3]. Це положення має на меті зменшити ризики, пов’язані із зовнішніми підрядниками, та гарантувати, що всі учасники цифрового ланцюга відповідають високим стандартам кібербезпеки.

Особливе значення в DORA приділяється обміну інформацією між фінансовими установами. Регламент заохочує обмін знаннями про кіберзагрози та вразливості, щоб підвищити колективну стійкість фінансової системи ЄС [3]. Такий підхід дозволяє швидко ідентифікувати нові загрози та ефективно реагувати на них у партнерстві з іншими учасниками ринку.

DORA поширюється на широкий спектр фінансових установ, серед яких: банки, страхові та перестрахові компанії, інвестиційні фірми, платіжні установи, електронні грошові установи, постачальники послуг з обміну криптовалют, центральні контрагенти, центральні депозитарії цінних паперів, управляючі компанії інвестиційних фондів, а також постачальники ІКТ-послуг, що обслуговують фінансові організації [3]. Така широка сфера застосування забезпечує комплексний підхід до захисту фінансової інфраструктури від кіберзагроз.

У разі порушення вимог DORA до фінансових установ можуть бути застосовані серйозні санкції. Це можуть бути адміністративні штрафи, розмір яких визначається національними регуляторами, а також обмеження або заборона на надання певних послуг [3]. Крім того, регулятори можуть вимагати усунення порушень у встановлені терміни. Такі заходи спрямовані на забезпечення високого рівня відповідальності фінансових установ та стимулювання їхнього дотримання єдиних правил цифрової операційної стійкості.

2.4. Атака отруєння даних

Атаки на етапі навчання ML називаються атаками отруєння [1, 9]. Під час атаки отруєння даних [5, 9] зловмисник контролює підмножину навчальних даних, вставляючи або змінюючи навчальні зразки. У атаці отруєння моделі [10] зловмисник контролює модель та її параметри. Атаки з отруєнням даних можуть застосовуватися до всіх парадигм навчання, тоді як атаки з отруєнням моделі є найбільш поширеними у федеративному навчанні [11], де клієнти

надсилають локальні оновлення моделі на сервер, що обробляє вхідні дані, і в атаках на ланцюг поставок, де шкідливий код може бути доданий до моделі постачальниками технології моделі. Під федеративним навчанням тут мається на увазі метод машинного навчання, орієнтований на умови, в яких кілька суб'єктів (часто званих клієнтами) спільно навчають модель, при цьому дані, які використовуються для навчання, розподіляються децентралізовано. Це відрізняє його від машинного навчання, в якому дані зберігаються централізовано.

Перші атаки отруєння, виявлені в додатках кібербезпеки, були атаками на доступність проти генерації профілів хробака та класифікаторів спаму, які невибірково впливають на всю модель машинного навчання та, по суті, спричиняють атаку типу «відмова в обслуговуванні» для користувачів системи ШІ.

Атаки отруєння вважаються одними з найнебезпечніших серед атак на ШІ та можуть спричинити або порушення доступності, або порушення цілісності. Зокрема, атаки з порушенням доступності спричиняють деградацію моделі машинного навчання на всіх етапах, тоді як цільові та бекдорні атаки з отруєнням є більш прихованими та викликають порушення цілісності на невеликому наборі даних. Атаки отруєння використовують широкий спектр конкурентних можливостей, таких як отруєння даних, отруєння моделі, контроль міток, контроль вихідного коду та контроль тестових даних, що призводить до кількох підкатегорій атак отруєння. За моделлю загрози вони можуть використовуватись як у сценаріях білої скриньки, так і чорної скриньки [18], що були розглянуті в розділі 1.3 цієї статті.

Серед методів запобігання атакам отруєння даних виділяють два найефективніші [1]:

• Очищення навчальних даних. Ці методи використовують той факт, що отруєні набори зазвичай відрізняються від звичайних навчальних наборів, які не контролюються зловмисниками. Таким чином, методи очищення даних призначені для очищення навчального набору та видалення отруєних наборів перед виконанням навчання машинного навчання.

• Надійне навчання. Альтернативним підходом до пом'якшення атак з порушенням доступності є модифікація алгоритму навчання ML і проведення надійного навчання замість звичайного навчання. У кількох статтях визначено методи надійної оптимізації, такі як використання функції скорочених втрат [20] або випадкове згладжування для додавання шуму під час навчання [21].

2.5. Стандарти PCI DSS та їх особливості

Payment Card Industry Data Security Standard (PCI DSS) – це міжнародний стандарт безпеки, розроблений для захисту даних власників платіжних карток [4]. Його головною метою є забезпечення безпечного середовища для обробки, зберігання та передавання даних про кредитні картки. Всі організації, які приймають, обробляють або зберігають дані платіжних карток, повинні дотримуватися вимог цього стандарту, щоб зменшити ризик несанкціонованого доступу, шахрайства та витоку конфіденційної інформації.

PCI DSS є універсальним набором вимог, обов'язковим для компаній різного масштабу: від невеликих Інтернет-магазинів до великих фінансових установ. Він сприяє зміцненню кіберстійкості компаній, які працюють у сфері електронних платежів, та формує довіру споживачів до цифрових транзакцій. Стандарт включає дванадцять головних умов, які разом забезпечують комплексний захист платіжної інформації [4].

Першою вимогою є захист систем, що обробляють платіжні дані, включаючи фізичний захист обладнання та програмного забезпечення. Це передбачає використання фаєрволів, сегментації мережі та інших заходів для запобігання несанкціонованому доступу. Друга вимога стосується захисту даних власників карток від стороннього доступу, зокрема шляхом шифрування даних як під час передавання, так і під час зберігання [4].

Також PCI DSS передбачає обов’язковий захист мереж, які обробляють дані про картки, від несанкціонованого доступу [4]. Це означає, що компанії повинні впроваджувати сучасні методи контролю доступу, моніторинг мережевого трафіку та системи виявлення вторгнень. Додатково стандарт вимагає захисту від шкідливого програмного забезпечення, яке може призвести до компрометації платіжних даних.

Суттєвою вимогою є обмеження доступу до платіжних даних: він має надаватися лише авторизованим користувачам, що мінімізує ризики внутрішніх загроз. PCI DSS також акцентує увагу на необхідності постійного тестування та розвитку безпеки систем, щоб своєчасно виявляти вразливості та запобігати можливим атакам [4].

Крім цього, компанії повинні впроваджувати та підтримувати діяльність ефективних політик безпеки, які встановлюють правила обробки платіжних даних та обов’язки працівників. Стандарт вимагає обмеження фізичного доступу до приміщень, де розміщене обладнання для обробки платіжних даних, а також постійного моніторингу інцидентів, які можуть свідчити про спроби несанкціонованого доступу [4].

PCI DSS наголошує на необхідності захисту від зовнішніх атак шляхом впровадження сучасних механізмів кіберзахисту, таких як системи виявлення вторгнень, міжмережеві екрани та антивірусні рішення [4]. Важливим є також управління підтримкою та обслуговуванням обладнання й програмного забезпечення, що передбачає регулярні оновлення систем та патч-менеджмент. Остання, але не менш важлива вимога – розробка та впровадження політик і процедур безпеки, які гарантують відповідність усім вимогам стандарту.

PCI DSS також запроваджує систему класифікації компаній за рівнями залежно від кількості оброблюваних транзакцій на рік [4]. Це дозволяє встановлювати різний рівень вимог до сертифікації залежно від обсягів діяльності. До першого рівня належать компанії, що обробляють понад 6 мільйонів транзакцій на рік, для яких передбачено найжорсткіші вимоги до безпеки. До другого рівня входять організації, що обробляють від 1 до 6 мільйонів транзакцій, а до третього – компанії з обсягом від 20 тисяч до 1 мільйона транзакцій на рік. Нарешті, до четвертого рівня належать компанії, які обробляють до 20 тисяч транзакцій щороку [4]. Такий підхід дозволяє гнучко адаптувати вимоги до різних бізнесів, одночасно забезпечуючи високий рівень захисту даних платіжних карток у всьому фінансовому ланцюгу.

3. Порівняння документів

3.1. Порівняння нормативно-правових документів ЄС

Для порівняльного аналізу нормативно-правових документів ЄС було обрано наступні критерії:

- мета регулювання;
- категорії суб’єктів регулювання;
- обов’язки організацій;
- вимоги до кібербезпеки;
- санкції за порушення;
- взаємозв’язки між документами.

Результати порівняння наведено у таблиці 1.

Таблиця 1 – Порівняння нормативно-правових документів ЄС за критеріями

Table 1 – Comparison of EU Regulatory Documents Based on Criteria

Критерій Criteria	**GDPR**	**DORA**	**NIS2**	**PCI DSS**
Мета регулювання **The purpose of regulation**	Захист персональних даних фізичних осіб у межах ЄС Protection of personal data of individuals within the EU	Забезпечення цифрової стійкості фінансових установ до ІКТ-ризиків Ensuring the digital resilience of financial institutions to ICT risks	Підвищення рівня кібербезпеки мережевих та інформаційних систем в ЄС Enhancing the cybersecurity level of network and information systems in the EU	Забезпечення безпеки даних платіжних карток Ensuring the security of payment card data
Категорії суб'єктів **Categories of subjects**	Усі організації, що обробляють персональні дані громадян ЄС All organizations that process personal data of EU citizens	Фінансові установи та ІКТ-постачальники, що працюють з ними Financial institutions and ICT providers working with them	Суб'єкти з «високим ступенем критичності», включаючи цифрові, енергетичні, медичні, транспортні сектори Entities with a high degree of criticality, including the digital, energy, healthcare, and transport sectors	Організації, які обробляють, передають або зберігають платіжні карткові дані Organizations that process, transmit, or store payment card data
Обов'язки організацій **Responsibilities of organizations**	Законна обробка даних, обмеження мети, мінімізація, точність, захист Lawful data processing, purpose limitation, data minimization, accuracy, protection	Управління ІКТ-ризиками, інцидент-репортинг, тестування, управління ризиками третіх сторін ICT risk management, incident reporting, testing, third-party risk management	Управління ризиками, звітування про інциденти, оцінка постачальників, відповідальність керівництва Risk management, incident reporting, supplier assessment, management accountability	Забезпечення 12 основних умов безпеки, включаючи шифрування, контроль доступу, моніторинг Ensuring 12 core security requirements, including encryption, access control, and monitoring
Вимоги до кібербезпеки **Cybersecurity requirements**	Забезпечення конфіденційності, цілісності й доступності даних Ensuring the confidentiality, integrity, and availability of data	Впровадження ІКТ-безпеки: виявлення, захист, реагування, відновлення, аудит Implementation of ICT security: detection, protection, response, recovery, audit	Впровадження технічних, організаційних заходів, тестування, безперервність бізнесу Implementation of technical and organizational measures, testing, and business continuity	Технічні та організаційні заходи для захисту даних платіжних карт та систем, що їх обробляють Technical and organizational measures to protect payment card data and the systems that process them

Санкції за порушення **Sanctions for violations**	До 20 млн. євро або до 4% світового обороту Up to €20 million or up to 4% of global turnover	Залежно від рішення національного регулятора: штрафи, обмеження діяльності, вимога усунення порушень Depending on the decision of the national regulator: fines, activity restrictions, requirement to eliminate violations	Адміністративні санкції, потенційна відповідальність керівників організації Administrative sanctions, potential liability of the organization's executives	Санкції від платіжних систем, відключення від обробки платежів, фінансові штрафи Sanctions from payment systems, disconnection from payment processing, financial penalties
Взаємозв’язки між документами **Interrelationships between documents**	GDPR фокусується на персональних даних, може доповнювати NIS2 або DORA GDPR focuses on personal data and can complement NIS2 or DORA	Може перетинатися з NIS2 (особливо в аспектах кібербезпеки) і з GDPR (якщо йдеться про персональні дані) May overlap with NIS2 (especially in cybersecurity aspects) and with GDPR (when personal data is involved)	Поширюється на ті самі галузі, що й DORA, та взаємодіє з GDPR у частині інцидентів і даних Applies to the same sectors as DORA and interacts with GDPR in terms of incidents and data	Може доповнювати GDPR щодо захисту фінансових персональних даних; має спільні цілі з DORA/NIS2 May complement GDPR in protecting financial personal data; shares common goals with DORA/NIS2

3.2. Порівняння нормативно-правових документів за впливом на бізнес та IT-інфраструктуру

GDPR в першу чергу впливає на організаційні процеси, змушуючи компанії переглянути політики конфіденційності, налагодити механізми для обробки запитів суб’єктів даних, наприклад: запити на доступ, виправлення чи видалення даних. Та призначити відповідального за захист даних. В IT-інфраструктурі це означає необхідність впровадження інструментів шифрування, анонімності, контролю доступу та логування. GDPR значно підвищує рівень захисту персональних даних, але майже не стосується фінансових транзакцій безпосередньо [2].

На відміну від GDPR, DORA зосереджується на цифровій стійкості фінансових організацій. Він впливає на бізнес через потребу в управлінні ІКТ-ризиками, регулярному тестуванні готовності до інцидентів, а також у створенні механізмів реагування та відновлення. Компанії повинні укладати чіткі контракти з IT-постачальниками, забезпечувати безперервність бізнесу навіть у разі кібератак або технічних збоїв. З технічного боку, це означає впровадження систем моніторингу, автоматизованих тестів безпеки, резервного копіювання, сегментації мереж тощо. DORA опосередковано посилює захист і персональних, і фінансових даних завдяки покращенню стійкості систем [2, 3].

Директива NIS2 також має значний вплив на організаційну структуру компаній, особливо тих, що належать до критично важливих секторів. Вона вимагає системного підходу до управління кіберризиками, створення інцидент-менеджменту, безпеки ланцюгів постачання, а також прямої відповідальності керівництва за впровадження кіберзахисту. В

IT-інфраструктурі це призводить до запровадження засобів моніторингу, журналювання, тестування безпеки, а також процедур забезпечення безперервності бізнесу. Як результат, посилюється захист як персональних, так і фінансових даних у рамках загальної кібербезпеки [1].

PCI DSS безпосередньо впливає на компанії, які працюють із платіжними картками. Він вимагає стандартизації процедур обробки платіжних даних, впровадження політик безпеки, обмеження доступу, фізичного захисту обладнання, а також регулярного тестування безпеки. В IT-сфері компанії повинні забезпечити шифрування даних карток, встановлення брандмауерів, систем виявлення вторгнень, обмеження доступу до систем. PCI DSS безпосередньо націлений на захист фінансових транзакцій та даних власників карток, забезпечуючи надійність платіжної інфраструктури [1].

4. Міжнародні аналоги нормативно-правових актів ЄС

Регуляторна система Європейського Союзу у сфері цифрової безпеки вважається однією з найрозвиненіших у світі. Водночас важливо зазначити, що багато інших країн та міжнародних організацій створили власні нормативні документи, які за своєю метою, структурою та принципами є подібними до європейських.

Зокрема, регламент GDPR, що встановлює єдині правила захисту персональних даних у межах ЄС, має численні відповідники у законодавствах інших країн. У США діють кілька галузевих актів, таких як HIPAA – закон про захист персональних медичних даних, який містить вимоги щодо безпеки інформаційних систем у сфері охорони здоров'я [5]. Для освітнього сектору розроблено FERPA, що гарантує студентам і їхнім батькам право на доступ до освітніх записів та їхнє коригування [6]. Водночас в окремих штатах запроваджуються ширші закони про конфіденційність, зокрема CCPA у Каліфорнії, що дає споживачам право знати, які персональні дані збираються про них, і вимагати їх видалення [7]. У Південній Америці Бразилія прийняла закон LGPD, який вважається майже повним аналогом GDPR – як за принципами обробки даних, так і за правами користувачів [8]. Окрему роль відіграє Конвенція № 108 Ради Європи, до якої приєдналася і Україна, – вона є першою міжнародною угодою, що встановила обов'язкові правила щодо захисту персональних даних як у державному, так і приватному секторах [9].

Регламент DORA, спрямований на забезпечення цифрової стійкості фінансового сектору ЄС, також має функціональні аналоги. У США Міжбанківська координаційна рада розробила FFIEC Cybersecurity Assessment Tool – інструмент для оцінювання рівня кіберзахищеності фінансових установ [10]. Структурно близькою до DORA є і модель NIST Cybersecurity Framework, яка охоплює повний життєвий цикл безпеки: від ідентифікації загроз до відновлення після інцидентів [11].

Директива NIS2, яка зобов'язує операторів критичної інфраструктури впроваджувати кіберзахист, має численні відображення у регулюваннях інших країн і сфер. Найбільш очевидною паралеллю є NIST Cybersecurity Framework у США, який є універсальним інструментом для підвищення кіберстійкості організацій [10]. У галузі енергетики в США та Канаді застосовуються стандарти NERC CIP – обов'язкові норми безпеки для енергетичних компаній [12]. Велика Британія після виходу з ЄС ухвалила UK NIS Regulations – документ, що фактично є національною адаптацією європейської директиви NIS [13]. До найближчих до NIS2 за ініціативами документів також можна віднести міжнародний стандарт ISO/IEC 27001, який стосуються управління інформаційною безпекою та забезпечення безперервності діяльності [14].

У сфері платіжних систем міжнародний стандарт PCI DSS знаходить чіткі відповідники у низці документів. Зокрема, ISO/IEC 27001 як базовий стандарт управління інформаційною

безпекою часто використовується у фінансовому секторі [14]. У США подібну функцію виконують рекомендації NIST SP 800-53 та 800-171 – це комплексні каталоги технічних, фізичних і адміністративних заходів захисту інформаційних систем [15, 16]. У галузі електронної комерції та хмарних послуг активно використовується стандарт SOC 2, що дозволяє оцінити рівень безпеки, конфіденційності та моніторингу в компаніях, які обробляють дані клієнтів [17].

Загалом, міжнародна практика демонструє, що ключові принципи цифрової безпеки – управління ризиками, прозорість, захист персональних даних, відповідальність організацій – стали універсальними.

5. Висновки

1. У дослідженні проаналізовано основні нормативно-правові документи ЄС у сфері кібербезпеки: Директиву NIS2, Регламент GDPR, Регламент DORA та стандарт PCI DSS.

2. Усі ці документи спрямовані на посилення кіберстійкості та цифрової довіри в ЄС, але мають різні акценти:

- NIS2 фокусується на безпеці мережевих та інформаційних систем, зокрема для критичної інфраструктури.
- GDPR створює систему захисту персональних даних, встановлює права громадян і правила обробки інформації.
- DORA регулює цифрову стійкість фінансового сектору, зокрема управління ІКТ-ризиками.
- PCI DSS встановлює вимоги до безпеки обробки платіжної інформації, особливо для e-commerce компаній.

3. Також документи мають багато точок перетину:

- GDPR доповнює NIS2 і DORA у питаннях захисту персональних даних під час кіберінцидентів.
- DORA і NIS2 мають спільні вимоги щодо управління ризиками та кіберстійкості.
- PCI DSS виступає як практичний інструмент реалізації вимог з безпеки платіжних даних, що підкріплює цифрову безпеку загалом.

4. Ефективне впровадження цих документів у країнах-членах ЄС сприятиме: підвищенню кіберстійкості; зміцненню довіри до цифрових технологій; сталому розвитку цифрової економіки; закріпленню позицій ЄС як глобального лідера у сфері цифрової безпеки.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

References

1. Directive (EU) 2022/2555 of the European Parliament and of the Council (2022) On measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union. – URL: https://surl.li/xpktzi
2. Regulation (EU) 2016/679 of the European Parliament and of the Council (2016) On the protection of natural persons with regard to the processing of personal data (GDPR). Official Journal of the European Union. – URL: https://surl.lt/zdilhe
3. Regulation (EU) 2022/2554 of the European Parliament and of the Council (2022) On digital operational resilience for the financial sector (DORA). Official Journal of the European Union. – URL: https://surl.li/lvfsva

4. PCI DSS Certification (n.d.) Payment Card Industry Data Security Standard. PCI Security Standards Council. – URL: https://getpci.com/
5. Centers for Medicare & Medicaid Services (n.d.) HIPAA – Health Insurance Portability and Accountability Act. – URL: https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification/hipaa
6. U.S. Department of Education (n.d.) What is FERPA? – URL: https://surl.lu/oizpnq
7. Office of the Attorney General of California (n.d.) California Consumer Privacy Act (CCPA). – URL: https://oag.ca.gov/privacy/ccpa
8. Brazilian Government (n.d.) General Personal Data Protection Act (LGPD). – URL: https://lgpd-brazil.info/
9. Council of Europe (1981) Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. – URL: https://ippi.org.ua/vid-redaktsiinoi-kolegii-konventsiya-%E2%84%96-108-radi-%D1%94vropi-%E2%80%9Cpro-zakhist-osib-u-zv%E2%80%99yazku-z-avtomatizovano
10. Federal Financial Institutions Examination Council (FFIEC) (n.d.) Cybersecurity Assessment Tool. – URL: https://www.ffiec.gov/resources/cat
11. Federal Trade Commission (n.d.) What is the NIST Cybersecurity Framework? – URL: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework
12. North American Electric Reliability Corporation (n.d.) Critical Infrastructure Protection (NERC CIP). – URL: https://www.techtarget.com/searchsecurity/definition/North-American-Electric-Reliability-Corporation-Critical-Infrastructure-Protection-NERC-CIP
13. UK Government (2018) The Network and Information Systems Regulations 2018 (NIS Regulations 2018). – URL: https://surl.li/zahavi
14. ISO/IEC (2022) ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection. – URL: https://www.iso.org/standard/27001
15. National Institute of Standards and Technology (2020) NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
16. National Institute of Standards and Technology (2020) NIST Special Publication 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
17. Palo Alto Networks (n.d.) What is SOC 2 Compliance? – URL: https://www.paloaltonetworks.com/cyberpedia/soc-2

RESEARCH AND COMPARISON OF EUROPEAN UNION REGULATORY DOCUMENTS IN CYBERSECURITY

Maryna Yesina[1,2], Candidate of Technical Sciences, Associate Professor, Acting Head of the Department of Cybersecurity of Information Systems, Networks and Technologies, Institute of Cyber Security and Artificial Intelligence, Research Associate-Consultant, JSC «Institute of Information Technologies»; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1137-2382
Yelyzaveta Lohachova[1], 5th year student at the Department of Cybersecurity of Information Systems, Networks and Technologies, Institute of Cyber Security and Artificial Intelligencer; e-mail: lohachova2020kb11@student.karazin.ua; ORCID: https://orcid.org/0000-0002-9815-466X
Ievgeniia Kolovanova[1], Candidate of Technical Sciences, Acting Deputy Director of Educational Work, Institute of Cyber Security and Artificial Intelligence; e-mail: e.kolovanova@karazin.ua; ORCID: https://orcid.org/0000-0002-0326-2394
[1] *V. N. Karazin Kharkiv National University, Ukraine*
[2] *JSC "IIT", Ukraine*
Manuscript was received March 1, 2025; Received after review April 1, 2025;
Accepted May 2, 2025

Abstract. The article presents a thorough study and comparison of the main regulatory acts of the European Union in the field of cybersecurity, including: NIS2 Directive, General Data Protection Regulation (GDPR), Digital Operational Resilience Regulation (DORA) and PCI DSS standard. These documents are considered fundamental elements in shaping the EU's current policy on digital information protection, covering personal data, financial information and critical infrastructure. The paper outlines the key objectives of each of the acts, analyses their scope of application, requirements for regulated entities, risk management mechanisms, incident reporting, interaction with suppliers, and sanction provisions. Particular attention is paid to comparing the acts in terms of their impact on business and IT infrastructure, as well as identifying the interrelationships between them. It has been established that although each document has its own focus - personal data protection, financial infrastructure resilience, digital network security, or payment card transaction protection - they are all aimed at creating a comprehensive cyber security ecosystem within the EU. The article also analyses international analogues of these acts, such as GDPR-like laws in the United States and Brazil, NIST and ISO standards, which demonstrates the global nature of the digital security problem and the search for common approaches to solving it. In conclusion, the paper emphasises the importance of a comprehensive and harmonised approach to cybersecurity as a key condition for the sustainable development of a digital society. Given the current threats, in particular geopolitical conflicts and the growing scale of cybercrime, the effective implementation of European standards is of particular importance for partner countries, in particular Ukraine, which needs to adapt the relevant standards to enhance national cyber resilience.

Keywords: *regulatory documents, European Union, regulatory documents, cybersecurity, business, information protection*

Conflicts of Interest: the authors declare no conflict of interest.

Електронне наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
№ 1(27) 2025

Міжнародний електронний науково-теоретичний журнал

Українською та англійською мовами

Комп'ютерне верстання – Єсіна М.В., Власова В.В.

Підписано до розміщення 30.06.2025. Гарнітура Times New Roman.
Ум. друк. арк. 4,43. Обсяг 5,5 Мб. Зам. № 21/25.

Харківський національний університет імені В. Н. Каразіна,
61022, м. Харків, майдан Свободи, 4.
Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.2009